

网络安全和信息化

(原《网络运维与管理》)

2017

超值
精华本

基础设施管理 系统维护
信息安全 故障诊断

《网络安全和信息化》杂志社 编



基础设施
管理

本板块以大量精彩详实的文章，为广大网络管理人员管理和维护网络提供了鲜活的实例和参考，帮助网络管理技术人员完成从网络管理菜鸟到高手的转变。



系统维护

本板块以数十篇精彩的实例文章，剖析在操作系统和应用软件使用过程中的解决方案，为网管员在操作系统和应用软件的配置和管理提供了众多方法和技巧。



信息安全

本板块以几十篇网络安全的实用性和应用性文章呈现给广大的读者，帮助读者朋友从容应对网络安全方面的问题。



故障诊断

本板块收集了《网络安全和信息化》杂志2016年在故障诊断栏目中的精华文章和优秀专题，既是网管员在日常工作中排查故障的工具手册，也是网管员提高网络管理水平的技术宝典。



中国工信出版集团



电子工业出版社
PUBLISHING HOUSE OF ELECTRONICS INDUSTRY
http://www.phei.com.cn

网络安全和信息化

2017

超值
精华本

(原《网络运维与管理》)

《网络安全和信息化》杂志社 编

电子工业出版社
Publishing House of Electronics Industry
北京·BEIJING

内容简介

《网络安全和信息化》(原《网络运维与管理》)是面向网络技术管理人员的实用性刊物。本书是2016年《网络安全和信息化》各期内容的汇集,按照栏目分类进行汇总,内容详尽,使用、保留价值高。全书分为基础设施管理、系统维护、故障诊断和信息安全4大板块,精彩的技术文章,是广大网络管理人员不可多得的业务指导书。

本书读者对象以网络管理技术人员(网管员)为主,辐射网络主管、网络爱好者、准网管员和所有关注网络应用与网络事业发展的人士。

未经许可,不得以任何方式复制或抄袭本书之部分或全部内容。
版权所有,侵权必究。

图书在版编目(CIP)数据

网络安全和信息化2017超值精华本:原《网络运维与管理》/《网络安全和信息化》杂志社编. — 北京:电子工业出版社,2017.5

ISBN 978-7-121-31177-2

I. ①网… II. ①网… III. ①计算机网络—网络安全 IV. ①TP393.08

中国版本图书馆CIP数据核字(2017)第063973号

策划编辑:符隆美

责任编辑:徐津平

特约编辑:顾慧芳

印刷:北京京科印刷有限公司

装订:三河市良远印务有限公司

出版发行:电子工业出版社

北京市海淀区万寿路173信箱

邮编:100036

开本:850×1168 1/16 印张:27.25 字数:1134千字

版次:2017年5月第1版

印次:2017年5月第1次印刷

印数:4000册 定价:89.00元

凡所购买电子工业出版社图书有缺损问题,请向购买书店调换。若书店售缺,请与本社发行部联系,联系及购电话:(010)88254888,88258888。

质量投诉请发邮件至zlt@phei.com.cn,盗版侵权举报请发邮件至dbqq@phei.com.cn。

本书咨询联系方式:010-51260888-819,faq@phei.com.cn。

FOREWORD 前言

《网络安全和信息化》（原《网络运维与管理》）杂志作为一本网络管理技术人员的专业杂志，长期以来一直以帮助企业提高IT基础设施运营水平、提高企业网络人员的管理水平为目标和宗旨，为企业的网络技术人员提供了一个技术和经验的交流平台，成为在网络管理技术人员中颇具影响力的IT专业媒体。为了更好地帮助广大网络技术人员提高网络管理水平，《网络安全和信息化》杂志特别推出《网络安全和信息化2017超值精华本》，内容包括2016年《网络安全和信息化》杂志基础设施管理、系统维护、故障诊断和信息安全栏目中所有精彩文章的汇总。

基础设施管理

对于广大网络管理人员来说，网络设备的管理和维护是他们最重要的工作之一，基础设施管理以大量精彩详实的文章，为广大网络管理人员管理和维护网络提供了鲜活的实例和参考，能够帮助网络管理技术人员完成从网络管理菜鸟到高手的转变。

系统维护

操作系统和各种应用程序的配置和管理，是网管员的又一项重要工作，系统维护以数十篇精彩的实例文章，剖析在操作系统和应用程序使用过程中的解决方案，为网管员在操作系统和应用程序的配置和管理提供了众多方法和技巧。

故障诊断

收集了《网络安全和信息化》杂志2016年在故障诊断栏目中的精华文章和优秀专题，既是网管员在日常工作中排查故障的工具手册，也是网管员提高网络管理水平的技术宝典。

信息安全

网络安全是网管员在日常工作中关注的重点，信息安全以几十篇网络安全的实用性和应用性文章呈现给广大的读者，帮助读者朋友从容应对网络安全方面的问题。

读者服务

轻松注册成为博文视点社区用户（www.broadview.com.cn），您即可享受以下服务。

提交勘误：您对书中内容的修改意见可在【提交勘误】处提交，若被采纳，将获赠博文视点社区积分（在您购买电子书时，积分可用来抵扣相应金额）。

与作者交流：在页面下方【读者评论】处留下您的疑问或观点，与作者和其他读者一同学习交流。

页面入口：<http://www.broadview.com.cn/31177>

二维码：



本书编委会

主 编：张碧薇

编 委：季 莹 赵志远

第1章 基础设施管理

利用软件搭建网络平台.....	2
网络运维简介.....	2
开源网络运维软件简介.....	2
治安监控综合实施方案.....	3
项目背景.....	3
项目实施方案.....	3
项目实施规划.....	4
EPON配置.....	4
后期维护.....	5
利用工具建立监控模型.....	5
一般网络流量监控使用的方法和技术.....	5
Sniffer Pro监控网络流量模型.....	6
日志审计分析系统的应用.....	7
利用端口聚合增加交换网带宽.....	8
端口聚合.....	8
流量平衡.....	9
服务器上使用随身WiFi.....	9
双网卡同时访问的设置方式.....	10
网络虚拟化技术的应用研究.....	11
技术概况.....	11
网络虚拟化在吐哈信息网的应用.....	11
IRF网络虚拟化技术的应用研究.....	11
结语.....	12
端口隔离在网络管理中的应用.....	13
联网计算机相互隔离的方法.....	13
单交换机端口隔离的实现.....	13
跨交换机端口隔离的实现.....	13
分组隔离.....	14
国际EPC项目的网络规划.....	14
项目背景.....	14
总体设想与规划方案.....	14
网络配置与网络参数设置.....	15
应用历程以及实施情况.....	15
实施中的难点与注意事项.....	16
如何解决IP地址故障.....	16
DHCP Snooping和ARP Detection技术介绍.....	16
具体配置方法和命令.....	17

功能验证.....	17
全网数据设备自动备份.....	17
自动备份软件实现原理.....	17
自动备份开发要点.....	18
自动备份相关服务安装事项.....	19
防火墙的配置.....	19
应用实例.....	19
综述.....	20
巧用NQA联动解决故障.....	20
工作流程.....	21
结语.....	21
系统网络端口安全防护.....	21
常用端口及分类.....	21
查看本机开放的端口.....	22
关闭本机不用的端口.....	22
重定向本机默认端口,保护系统安全.....	22
思科交换机架构探讨.....	23
Cisco 6500系列交换机体系架构.....	23
背板与机箱槽位间的数据通路.....	24
Cisco常用线卡.....	26
常用线卡结构图.....	26
线卡间的数据包流向.....	27
结语.....	28
链路聚合扩带宽.....	28
巧用批处理查找端口.....	30
实现思路.....	30
链路聚合在局域网的应用.....	33
物理层连接.....	34
数据配置.....	34
验证效果.....	34
注意事项.....	35
简化版的网络防火墙.....	35
在核心上对指定VLAN做ACL控制.....	35
在接入层交换机上做ACL控制.....	35
用命令配置两张网卡.....	36
4KB扇区硬盘安装之路.....	36
如何延长UPS的使用寿命.....	37
负载数量应适中.....	37

感性负载不搭接	37	企业外包呼叫中心的保护技术	54
定期维护是保证	38	项目背景	54
工作环境要讲究	38	接入ISP网络保护设计	54
快速破坏环路	38	内部网络保护设计	55
二层环路危害	38	结语	56
二层环路产生原因	38	多点视频会议连接方式比较	56
环路检测原理及报文结构	39	校园无线平台构建研究	57
环路检测功能配置方法(以华为交换机为例) ...	39	中学校园无线网络规划与设计原则	58
Mac在Windows上的打印	41	案例背景及需求分析	58
对Windows PC进行配置	41	曲靖市某中学校园无线网络设计	58
配置你的Mac	41	网络仿真测试数据及其分析	59
寻找丢失的交换机	42	结语	59
批处理实现信息统计	43	快速实现多系统集中维护	60
设计思路	43	维护现状概述	60
常用命令及实现	43	集中维护多元设备方案介绍	60
批处理脚本	43	维护台的设置	61
结语	44	结语	62
浅谈ACL在SSH中的应用	44	巧用交换机的局域网业务	63
无线局域网部署的优化	45	VLAN简述	63
交叉板故障处理及分析	47	交换机接口类型	63
网络拓扑	47	Hybrid接口转发数据帧的原理	63
故障经过	47	应用Hybrid特性区分局域网业务实例	63
故障处理	47	结语	64
故障分析	47	多网段监控网络聚合方法	65
维护经验及改进措施	47	PC多网卡法	65
浅析高校无线网络的部署	48	网络考试Kiosk模式的探究	66
高校无线网络的需求分析	48	网络考试现状	66
高校无线网络的部署策略	49	问题的提出	66
结语	50	问题的解决	67
双绞线系统中问题的解决	50	浅析策略路由的使用	67
什么是近端串扰	50	ACL在网络中的应用	69
近端串扰过大的原因	50	网络打印新经验	71
近端串扰过大的影响	51	在Windows中快速安装共享打印机	71
解决近端串扰过大需要注意的方面	51	将网络打印机添加为Windows系统本地打印机 ...	71
结语	52	为笔记本设置“对位”打印	71
解决网络规划中的问题	52	通过第三方软件管理网络打印	71
某政务中心Internet网络接入规划问题	52	使用虚拟打印机	71
某单位通过VPN网络之后路由器信息没有更新 ...	53	手机和平板电脑也能“网打”	72

网络设备数据采集与分析.....	72	通过PE查电脑IP地址.....	92
局域网无线路由设置方法.....	73	Hyper-V集群生成问题对策.....	93
无线路由器的一般设置方法.....	73	Hyper-V Hosts与VMM Host Group.....	93
特殊情况下无线路由器的设置方法.....	75	Hyper-V 共享型存储.....	93
克隆MAC地址.....	75	Hyper-V主机的网络化需求.....	94
无线路由器的安全策略.....	75	用Virtual Machine Manager生成Hyper-V集群.....	94
结语.....	76	ARP代理解决地址重叠.....	95
第2章 系统维护		网络结构.....	95
Exchange群集复制配置与管理.....	78	改造计划.....	95
架构准备与基础设置.....	79	故障现象.....	96
CCR仲裁与服务角色设置.....	80	故障分析.....	96
备用群集设置与最终测试.....	81	故障解决.....	96
结语.....	82	经验总结.....	96
升级vSphere实例.....	82	服务器操作系统巧安装.....	97
升级的主要流程.....	83	准备篇.....	97
当前主机.....	83	方案篇.....	97
升级vCenter Server 5.5到6.0.....	83	制作篇.....	98
升级vSphere Client.....	84	维护篇.....	99
安装vCenter Server Update Manager.....	84	部署高可靠性ACS主备机.....	99
启用Update Manager插件.....	85	配置ACS主机.....	100
升级ESXi主机.....	85	配置ACS备机.....	100
被忽视的远程管理模块.....	87	同步数据库.....	101
更改远程管理口的IP地址.....	88	让View 6.1支持XP.....	101
更改远程管理默认用户USERID的密码,		快速备份与迁移虚拟机.....	102
或者创建新用户.....	88	准备工作.....	102
使用远程管理功能.....	88	开启Hyper-V复制功能.....	102
经验总结.....	89	开始备份副本.....	103
用复制功能实现灾备.....	89	启用计划转移.....	104
测试环境.....	90	Windows 7 中使用工作文件夹.....	104
配置副本服务器.....	90	应用需求.....	105
启用复制.....	90	同步设置.....	105
配置主服务器.....	91	批处理统计信息.....	106
测试部署.....	91	设计思路.....	106
测试故障转移.....	91	常用命令及实现.....	106
经验总结.....	92	批处理脚本.....	106
		经验总结.....	107
		删除孤立的虚拟机.....	107
		登录View Composer删除孤立的虚拟机.....	107

登录View连接服务器删除数据库.....	108	让虚拟服务器时间同步.....	121
修改Manifest控制权限.....	108	应用环境.....	121
用户账户控制机制.....	108	时间同步需求.....	121
修改Manifest文件.....	109	配置实现.....	121
注意事项.....	110	应用效果.....	122
部署vCenter Server经验.....	110	为Windows 2012指定授权服务器.....	122
部署 vCenter Server Appliance时的“客户		安装远程桌面会话主机.....	123
端集成插件”问题.....	110	修改本地策略指定授权服务.....	123
更改vCenter SSO的密码策略.....	110	修改组策略指定授权服务.....	123
vCenter升级问题.....	111	用AppLocker设置控制策略.....	124
vSphere Web Client英文界面问题.....	111	在Windows Server 2012 R2中配置AppLocker..	124
显示ESXi的正常运行时间为0秒.....	111	利用AppLocker阻止用户安装程序实例.....	124
在IE11不能初始配置VDP 5.5.x及VDP 6.0的问题.....	112	经验总结.....	125
调整Linux系统CPU频率.....	113	桌面虚拟化构建电教室.....	125
用VHD打造双系统.....	114	传统教室多媒体系统存在的问题.....	125
将Hyper-V安装到Windows 10.....	115	桌面虚拟化技术分析.....	125
Hyper-V安装条件.....	115	桌面虚拟化的优势.....	126
适用系统.....	115	实施方案.....	126
安装Hyper-V操作.....	115	经验总结.....	126
值得关注的ReFS.....	116	虚拟云桌面管控终端.....	127
ReFS:可靠可扩展的磁盘结构.....	116	应用需求.....	127
ReFS的局限性.....	116	解决方案.....	127
ReFS v2有哪些改进.....	116	构建Web日志分析服务器.....	128
用Linux日志运维服务器.....	117	Web日志分析服务器部署方法.....	128
Linux系统运维难点.....	117	Web日志分析原理.....	128
日志文件.....	118	部署rsync.....	129
日志文件应用实例.....	118	定时执行工具cron.....	130
Windows 10 实用技巧.....	119	日志分析工具——AWStats.....	130
重置Windows背景.....	119	用KVM虚拟化网络服务.....	131
修改Windows 10主题色.....	119	安装配置KVM服务器.....	131
升级到Windows 10之后如何删除旧系统冗余文件.....	119	转化物理机为KVM虚拟机.....	132
关闭Windows 10操作中心.....	120	安装配置远程管理工具.....	133
解决Windows 10下IE运行时频繁		经验总结.....	134
提示“Internet Explorer已停止工作”.....	120	管理Windows Server 2008文件服务器.....	135
禁用Windows 10的追踪功能.....	120	分布式文件系统(DFS).....	135
为Windows 10文件资源管理器“整容”.....	120	文件服务器资源管理.....	135
让Windows 10账户只能打开指定应用.....	120	打印机集中配置.....	135

初始化已使用的硬盘.....	139	经验总结.....	151
用组策略修改主页设置.....	139	构建收入合同管理系统.....	151
IE7主页不管用,修改组策略.....	139	建设背景.....	151
没有IE这一项怎么办.....	140	研究与实践.....	151
模板文件是什么.....	140	经验与体会.....	152
用Linux巧解硬盘逻辑锁.....	141	NTP服务统一终端配置.....	153
制作启动盘.....	141	可选的NTP方案.....	153
启动计算机.....	141	服务端建设方法设计.....	153
修复硬盘主引导记录.....	141	设置客户端.....	153
恢复硬盘数据.....	141	HPUX系统下NTP客户端设置.....	154
让虚拟机实现互动.....	142	Cisco网络、安全设备NTP客户端设置.....	154
Workstation连接到vSphere直接上传下载.....	142	华为网络设备NTP客户端设置.....	154
上传虚拟机.....	142	经验总结.....	154
下载虚拟机.....	143	在存储虚拟机迁移数据.....	155
在Workstation与vSphere中使用OVF文件交互.....	143	常见数据迁移技术.....	155
在vSphere中导出OVF.....	144	基于存储虚拟机的不停机数据迁移技术	
在vSphere中部署OVF模板.....	144	及迁移方案步骤.....	156
在Workstation中更改虚拟机硬件版本.....	144	数据迁移项目实践及效益评估.....	157
在Workstation中导出与导入OVF.....	145	结语.....	157
存储浏览器复制或下载.....	145	Exchange 2010邮件管理秘诀.....	158
从vSphere下载虚拟机.....	145	电子邮件发送前的审阅管理.....	158
将虚拟机上传到vSphere.....	145	如何解决E-mail存档的问题.....	159
向WinPE添加服务器驱动.....	146	电子邮件保留策略功能使用.....	159
WinPE调用磁盘阵列卡驱动程序流程.....	146	多重电子邮件邮箱审核管理.....	160
向WinPE系统添加磁盘阵列卡驱动程序.....	146	使用Exchange命令控制台管理多重邮箱的探索... ..	161
WinPE系统制作.....	146	如何在Outlook 2010中同时开启探索邮箱.....	161
使用DISM命令向WIM映像中添加驱动程序... ..	147	设置AD RMS主机集成Exchange Server 2010	162
经验总结.....	148	如何设置Exchange 2010服务器的IRM.....	162
监控远程用户行为.....	148	建立集成AD RMS传输规则.....	162
了解远程在线用户.....	148	自我测试小秘诀.....	163
限制远程桌面用户使用同一个会话.....	148	客户端电子邮件传送测试.....	163
在Windows Server 2012中实现允许多个		结语.....	163
用户远程桌面登录.....	148	FCoE在Linux下的部署.....	163
用Kickstart自动安装系统.....	149	FCoE的部署.....	164
自动安装需求.....	149	FCoE适配卡在Linux下配置.....	164
Kickstart自动安装原理.....	150	FCoE交换机配置.....	167
PXE协议.....	150	日志审计分析系统的应用.....	168
Kickstart网络自动化安装技术架构.....	150	数据库日志.....	168

操作系统日志	168	故障排查	190
网络及安全设备日志	169	故障解决	191
如何使用Oracle数据库分区表	169	经验总结	191
分区表与海量数据	169	使用重启大招之前的思索	192
分区表与数据归档	170	故障现象	192
分区表与RAC集群环境	170	系统介绍	192
如何实施分区	171	排错与测试	192
结语	171	经验总结	194
搭建Hadoop实验平台	171	图像编码器互联故障解析	194
实验材料	171	故障现象	194
实验过程	171	故障排查	194
经验总结	175	故障排除	195
利用ownCloud建立云盘	176	经验总结	195
为何选择ownCloud建立云盘	176	添加带外控制设备网不通	195
ownCloud的安装过程	176	故障现象	195
ownCloud的使用	177	故障排查	196
Hyper-v Replica功能详解	179	故障分析	196
测试环境	179	故障排除	196
测试步骤	179	电磁屏蔽机房维护记	196
结语	182	故障现象	196
搭建网络数据备份系统	182	故障排查	196
数据备份现状	182	故障解决	197
Rsync远程同步工具简介	183	经验总结	197
统一网络数据备份系统建设方案	184	360浏览器医生排除故障	197
结语	186	搞定IE浏览器无法登录网银账户	197
		12306订票网上支付报错	198
		经验总结	198
第3章 故障诊断		网关IP配置引发故障	199
设备升级欲速则不达	188	故障现象	199
故障现象	188	故障排查	199
故障分析	188	故障解决	200
故障解决	188	经验总结	200
经验总结	189	IRQ冲突硬件无法使用	200
探究网络同传延时故障	189	故障现象	200
故障现象	189	故障分析	200
故障排查	190	IRQ家族	201
故障处理	190	IRQ的分配	201
交换机级联端口被绑之后	190	IRQ冲突	201
故障现象	190		

CONTENTS

故障排查	201	重点突破	218
故障解决	202	经验总结	219
解析交换机CPU占用率	203	摆脱强制升级	219
交换机CPU占用率高的危害	203	故障现象	219
交换机CPU占用率高的正常应用场景	203	故障分析	219
故障引发交换机CPU占用率高	204	故障解决	220
CPU占用率高故障排除方法	204	用交换机监测网络环路	221
插错网线闹风暴	207	故障现象	221
故障分析	207	故障定位	221
排除步骤	207	故障排除	221
经验总结	208	经验总结	222
语音业务单通故障分析	208	超大硬盘服务器安装记	222
故障现象	208	故障现象	222
故障分析	208	故障分析	222
解决方法	209	故障解决	222
维护建议	209	配置详解	223
修复RedHat虚拟机挂盘故障	209	经验总结	223
故障现象	209	用交换机捕获数据排障	223
故障处理	210	数据包捕获环境与方式	224
故障原因分析	210	交换机自主捕获方式	225
经验总结	210	交换机自主捕获数据包示例	225
不可忽视电源线干扰	211	滥用飞秋网堵塞	225
故障现象	211	故障现象	225
故障排查	211	故障解决	226
故障分析	211	规范使用飞秋	226
经验总结	212	关注交换机版本	227
路由器IOS灾难恢复	212	故障现象	227
路由器IOS相关概念	212	故障分析	227
路由器IOS灾难恢复	212	试验验证	228
路由器IOS故障处置案例	214	故障启示	229
交换机端口不可用解析	215	被“*”感染的IP	229
故障现象	215	故障现象	229
故障原因	215	更换IP临时解决	229
故障解决方法	215	故障排查	229
广告代码为何无法解析	217	故障排除	230
故障现象	217	修复交换机系统文件	230
故障诊断	217	获取系统文件	230
全方位排查	218	网络启动	231

下载系统文件	231	策略路由缺失引发故障	242
修改交换机启动项设置	231	故障现象	242
低版本引发路由器重启	232	故障分析	242
故障现象	232	故障解决	242
引起路由器重启的主要原因	232	经验总结	242
故障分析	232	PoE供电引发故障	243
故障排除过程	232	故障现象	243
辨识真伪网关	233	故障排查	243
故障现象	233	故障分析	244
故障排查	233	设备供电流程	244
故障分析	234	故障解决	244
经验总结	234	经验总结	244
定位违规电脑	234	找回丢失的虚拟机	245
故障现象	234	故障现象	245
故障排查	235	故障排查	245
故障解决	235	故障解决	246
经验总结	235	经验总结	247
软件引起的开机故障	235	链路层协议为何报错	247
故障现象	235	网络结构	247
故障排查	235	故障解决	247
故障解决	236	经验总结	248
故障分析	236	精确定位“软故障”源头	249
经验总结	236	背景及故障现象	249
无效路由条目闹故障	237	故障分析	249
故障现象	237	故障解决	250
造成网络异常的可能原因	237	经验总结	250
故障排查	238	链路聚合解决网络瓶颈	251
经验总结	238	故障现象	251
限速配置引故障	239	故障排查	251
故障现象	239	解决方案	252
故障分析	239	配置交换机	252
故障解决	239	扩展应用	252
经验总结	239	用时钟反转调试路由	253
光模块选型不当网不通	240	网络结构	253
故障现象	240	路由调试过程	253
引起链路无法连通的可能原因	240	配置端口为异步工作方式	253
故障排查	240	配置时钟反转	254
经验总结	241	经验总结	254

CONTENTS

用事件查看器查故障.....	255	故障排查.....	266
Windows事件查看器的作用.....	255	故障排除与分析.....	267
事件查看器日志分类.....	255	修复网站服务器.....	267
事件查看器记录内容.....	255	故障现象.....	267
用事件查看器解决故障案例.....	256	故障排查.....	267
经验总结.....	256	故障排除.....	268
两网串连故障.....	257	经验总结.....	268
故障现象.....	257	被遗忘的路由.....	268
故障排查.....	257	故障现象及处理.....	269
经验总结.....	258	恢复测试.....	269
安装群集遇麻烦.....	258	故障分析.....	270
故障现象.....	258	经验总结.....	270
故障排查.....	258	抓出交换机系统Bug.....	270
故障解决.....	259	故障现象.....	270
硬盘扩容出故障.....	259	故障分析.....	271
故障现象.....	259	故障排查.....	271
故障处理.....	259	故障排除.....	272
经验总结.....	260	经验总结.....	272
巧破数据包重传故障.....	260	进水导致光纤链路异常.....	272
故障现象.....	260	故障现象.....	272
故障排查.....	261	网络不稳定因素.....	272
故障原因.....	261	故障排查.....	273
数据包重传解决方法.....	261	故障排除.....	273
组播路由故障排除心得.....	263	经验总结.....	273
故障现象.....	263	机房搬迁网不通.....	274
步骤一:查看局域网交换机能否接收到组播包... 263		故障现象.....	274
步骤二:检查路由自治系统间组播路由是否异常.. 263		故障排查.....	274
步骤三:检查RP之间能否建立MSDP对等体.... 264		故障排除.....	274
经验总结.....	264	故障分析.....	275
接口降级识别加密狗.....	264	经验总结.....	275
故障现象.....	264	无线路由引发网络故障.....	275
故障原因.....	264	网络环境.....	275
解决方案.....	264	故障现象.....	275
解决过程.....	264	故障排查.....	275
恢复办法.....	265	故障排除.....	276
关于USB Over Network.....	265	经验总结.....	276
路由汇聚引发网络故障.....	266	路由故障分析三例.....	277
故障现象.....	266	故障现象一.....	277

故障现象二	277	经验总结	287
故障现象三	277	HP小型机数据库故障处理	288
替换法解决存储问题	278	故障现象	288
故障现象	278	故障处理及分析	288
解决方案	278	经验总结	289
故障处理过程	278	防火墙故障排除案例	289
揭秘无线同频干扰	279	实例一:客户机无法Telnet或GUI管理防火墙 ..	289
故障现象	279	实例二:增加策略禁止某主机,该主机仍能	
故障分析	279	通过防火墙	290
故障排除	280	实例三:IP地址绑定未起作用	290
经验总结	281	实例四:使用防火墙后原本可互相访问的	
华为交换机互联出故障	281	主机无法通信	290
故障现象	281	经验总结	290
故障排查	281	寻找无线信号异常根源	291
故障排除	282	故障现象	291
故障分析	282	故障原因	291
经验总结	282	故障排除步骤	292
用流量统计追查丢包	282	经验总结	292
丢包故障点快速定位方法	282	HP服务器时间同步出Bug	293
流量统计定位原理	282	网络环境	293
流量统计部署方法	283	故障现象	293
二层丢包故障排除	283	故障排查	293
三层丢包故障排除	284	故障原因	294
经验总结	284	故障排除	294
设备兼容性带来的故障	284	经验总结	294
故障现象	284	新换电脑为何无法上网	294
故障分析	284	网络环境	294
故障排除	284	故障现象	294
故障总结	285	故障排查	295
排查High CPU网络故障	285	故障排除	295
故障现象	285	经验总结	296
故障排查	285	巧用CNA排除接线故障	296
故障排除	286	网络结构	296
经验总结	286	故障现象	296
配置失误导致监控异常	286	故障分析	296
故障现象	286	故障排查	297
故障排除	286	系统升级惹麻烦	298
故障原因分析	287	故障现象	298

故障排查	298
故障排除	298
经验总结	299
路由器兼容性故障案例	299
案例一:路由器协议不匹配	299
案例二:路由器时钟匹配问题	299
案例三:路由器带宽匹配问题	300
分析方法	300
NAT配置不当网异常	301
故障现象	301
故障分析	301
故障排除	302
经验总结	302
地址重复引发路由故障	303
故障现象	303
故障分析	303
故障排除	303
故障总结	304
当虚拟网关遇上地址冲突	304
故障因素	304
故障现象	305
故障排查	305
故障排除	305
故障分析	305
虚拟路由冗余协议	306
端口控制阻碍远程接入	306
故障现象	306
故障排查	306
故障分析	307
故障排除	307
经验总结	308
防火墙影响路由备份	308
故障现象	308
故障排查	308
故障排除	308
经验总结	308
VRRP引发网络中断	309
故障网络拓扑结构	309

故障现象	309
故障原因分析	309
故障排除	310
经验总结	310

第4章 信息安全

防共享,堵漏洞	312
防共享检测技术介绍	312
防共享设备的部署	313
结语	314
正确使用Cookies	314
Cookies及其功能	314
Cookies的主要安全隐患	315
确保Cookies安全措施	315
IP地址封堵有法	316
华为S9306的访问控制	318
定义访问控制列表ACL	318
创建流分类	318
创建流行为	318
创建流策略	318
应用流策略	319
IP扩展访问控制列表的配置	319
扩展访问控制列表配置方法	319
配置命名的访问控制列表	320
OpenSCAP管理主机安全	320
什么是SCAP	320
安装OpenSCAP软件包	321
使用Oscap 命令行工具	321
扫描本地系统	321
使用 SCAP工作台	322
使用SACP 工作台扫描系统	323
结语	323
关闭Windows系统危险端口	323
系统关闭法	323
TCP/IP筛选关闭法	324
IP安全策略关闭法	324
防火墙关闭法	325
经验总结	325

流媒体环境下的防火墙配置.....	326	不让漏网病毒潜藏.....	343
Windows Media服务器配置软件防火墙.....	326	多VLAN环境下防火墙配置.....	344
支持单播流配置防火墙.....	327	需求分析.....	344
支持多播流配置防火墙.....	327	配置方案.....	345
支持允许对防火墙之外的编码器进行访问.....	327	操作流程与步骤.....	345
支持允许分发服务器与源服务器的连接.....	328	访问控制策略失效案例.....	346
支持允许管理远程服务器.....	328	案例一:VLAN1透传引起的ACL策略失效.....	346
其他.....	328	案例二:DHCP改造引起的ACL策略失效.....	346
内网安全防护体系的设计.....	329	优化网络性能,细化安全配置.....	347
安全防护体系总体设计.....	329	网络与信息安全建设总体现状.....	347
安全策略设计.....	329	网络与信息安全建设存在的问题.....	348
网络VLAN划分及防火墙配置.....	330	网络与信息安全建设解决方法.....	349
服务器配置.....	330	驱逐病毒恢复IE活力.....	350
结语.....	330	电力企业中的病毒防护.....	352
巧设Event Viewer让AD更安全.....	331	电力企业病毒防护系统应当考虑的几个问题... 352	
让AD具有安全审计功能(Security Auditing) ... 331		多层次、分级式病毒防护体系的设计原理.....	353
定制安全显示.....	331	系统中心.....	353
通过Email接收安全警报.....	331	服务器端.....	353
主动配置,数据存取更安全.....	332	客户端.....	353
移除数据加密图标.....	332	Internet网关.....	353
拒绝解密威胁数据.....	332	“移动式”管理员控制台.....	353
追踪数据存取痕迹.....	333	病毒定义代码的更新策略.....	354
智能授予数据权限.....	333	病毒服务器的实时防护策略.....	354
管好数据安全证书.....	334	客户端的实时防护策略.....	354
谨防隐私数据显现.....	334	客户端的安装策略.....	354
Hadoop加密静态及传输数据.....	335	结语.....	355
Apache Hadoop传输加密.....	335	Intranet网络架构安全评估.....	355
RPC/SASL.....	335	Intranet网络架构安全评估方案.....	355
TCP/IP.....	336	网络建设规范性.....	355
TLS/HTTPS.....	336	网络可靠性.....	356
HDFS外的静态数据加密.....	336	网络边界安全性.....	356
移动设备安全使用全监控.....	337	网络协议安全分析.....	356
监控染毒状态.....	337	网络流量分析.....	356
监控本地状态.....	337	网络通信安全.....	356
监控远程状态.....	338	网络安全管理.....	356
SNMP服务弱口令安全漏洞防范.....	340	强化IIS 8.0安全性.....	357
让漏网病毒无力回天.....	341	终端账号安全不容忽视.....	359
寻找漏网病毒踪迹.....	341	监控账号创建安全.....	359

强制账号密码安全	360	让Web服务更安全	381
保障账号盗用安全	360	巧妙谢绝危险访问	382
严控账号权限安全	360	谢绝使用无线网络	382
管理隐藏账号安全	361	谢绝访问重要网站	382
保护CMD命令行安全	362	谢绝随意更改地址	383
利用NTFS权限,防止黑客操作CMD命令	362	谢绝使用有线网络	383
对CMD进行完美加密	362	谢绝进行Ping攻击	384
为CMD设置专用记录器	363	提高Linux安全技巧	384
莫让远控软件成帮手	363	多账户信息外泄防范	386
清除暗中潜伏的Radmin	364	预防跳转列表外泄	386
被黑客恶意控制的TeamViewer	364	预防特定程序外泄	386
无线路由安全不容忽视	365	预防登录账号外泄	387
更新固件程序	365	预防数据分区外泄	387
修改账号密码	366	预防磁贴记录外泄	388
调整远程端口	366	预防搜索功能外泄	388
预防网页劫持	367	预防文件历史外泄	389
拒绝他人蹭网	368	预防共享访问外泄	389
让木马无法藏身启动项	368	事前设防“做主”登录安全	389
值得注意的非常规启动位置	369	强化登录安全提醒	389
为启动项和服务安装“监控器”	369	严密监控登录状态	390
实战攻防TCP/IP筛选策略	370	强行使用登录密码	390
设置TCP/IP筛选策略	370	严格限制登录方式	391
黑客如何破解TCP/IP筛选策略	370	加强登录时间管控	392
彻底保护TCP/IP筛选策略	371	限制登录权限	392
交换机安全由配置把关	372	SSH转发保VNC安全	393
配置密码保护	372	VNC的基本功能与操作	393
配置环路保护	372	SSH的基本功能与操作	393
配置服务保护	373	使用SSH转发,为VNC开启加密通道	394
配置流量保护	373	加强无线网络安全性	394
配置VTP协议保护	374	无线网络安全机制	394
配置Root地位保护	374	无线安全面临的威胁	395
DHCP上动手脚,安全有保障	375	设置复杂密码 抗击非法破解	395
保护重要主机安全	375	抗击快速破解的技巧	396
保护网络运行安全	375	搭建VPN环境	396
保护终端接入安全	376	保护无线VPN的技巧	397
预防ARP欺骗攻击	377	Windows IP安全策略	398
让服务器网络更安全	378	移动设备安全靠策略	399
让DNS服务更安全	378	停用自动播放功能	399
让DHCP服务更安全	379	按需分配操作权限	399

安装特定移动设备	400	包过滤保障网络安全	406
禁用自动运行命令	401	避免单位网络单点风险	408
安全“例外”效率兼顾	401	网络信息安全建设总体现状	408
隔离“例外”让共享高效	401	网络信息安全建设不足之处	409
虚拟“例外”让升级高效	402	网络信息安全提升基本策略	409
扫描“例外”让杀毒高效	403	构建网络信息安全的意义	410
阻断“例外”让浏览高效	403	小心注入式入侵预防中的短板	411
拦截“例外”让运行高效	403	“短板”一：被“注入中转”注入的“防注”	411
重识“DNS劫持”	404	“短板”二：被搜索“出卖”的“伪静态”	411
什么是DNS	405	“短板”修补措施：做好三个“化”	412
什么是DNS劫持	405	构筑信息终端防护“安全之门”	412
什么是DNS污染	405	完善本地安全策略	412
解决方法	405	优化系统注册表设置	413
写在最后	406	制定IP安全策略	413
		打造更安全的远控服务	414

NetAdmin World 2017

第1章 基础设施管理

利用软件搭建网络平台

广东 王晓鹏

网络运维简介

网络运维，是指为保障电信网络与业务正常、安全、有效运行而采取的生产组织管理活动，简称运维管理或 OAM (Operation Administration and Maintenance)。网络运维需要对网络中防火墙、路由器、交换机、服务器、存储设备、电力系统、空调系统等设备进行实时监测。

由于学校网络建设时，大多采购多种品牌网络设备进行组合，以兼顾网络性能和资金投入，但同时也带进来网络运维工作的复杂性。虽然各种网络设备都自带管理平台，没有形成一个统一的整体，特别是数量众多的接入交换机和服务器，需要网络运维人员逐个登录查看的话，是比较繁杂琐碎的工作。

开源网络运维软件简介

由于商业软件的定制化成本比较高，建议有一定研发能力的单位都采用功能类似的开源网络运维软件进行整合和定制，以满足单位的个性化需求。

目前流行的开源网络运维软件主要有：

Cacti 是非常广泛的性能图形和趋势分析工具，可以用来追踪任何检测指标，并绘制在图表上。Cacti 是用 PHP 语言实现的一个软件，它的主要功能是用 SNMP 服务获取数据，然后用 RRDtool 储存和更新数据，当用户需要查看数据的时候用 RRDtool 生成图表呈现给用户。因此，SNMP 和 RRDtool 是 Cacti 的关键。SNMP 关系着数据的收集，RRDtool 关系着数据存储和图表的生成。

Nagios 能有效监控网络服务 (SMTP、POP3、HTTP、NNTP、Ping 等)、监控主机资源 (处理器负荷、磁盘利用率等) 和主机状态等。在系统或服务状态异常时发出邮件或短信报警第一时间通知网站运维人员，在状态恢复后发出正常的邮件或短信通知。

Icinga 是 Nagios 的分支，是一个介于 Nagios 社区版和企业版间的产品，完全兼容以前的 Nagios 应用程序

及扩展功能。特别将致力于解决 Nagios 项目现在的问题，比如不能及时处理 Nagios 项目的 Bug、新功能不能及时添加等。还有在新的 Icinga 项目中，将更好地实现数据库集成方面的功能，标准化第三发应用程序的接口等。中文化项目是由 Icinga 中文化项目组在 Icinga (<http://www.icinga.com>) 基础上针对中文需求进行优化及修改，同时集成 nagiosgraph 或 pnp4nagios 绘图，包括简体中文、繁体中文 (计划)，界面以及生成的图像都已中文化。

NeDi 是一款网络发现与配置工具，它省去了逐个 telnet 接入交换机，连续不断地扫描交换机上 MAC 地址表来执行 MAC 地址查找的麻烦，它可以发现编目设备，然后将数据转移到一个本地数据库内。可能没有其他工具那么出名，但这是追踪网络内设备的很棒的解决方案，它可以持续追踪网络基础设施和目录设备，监控其发现的一切东西。它可以提供所有设备的当前位置以及历史信息。可以用于定位被盗或丢失的设备，当这些设备重新出现在网络时它会提醒你。它甚至可以在地图上显示所有已知和发现的链接，显示每个网络互连的情况，到物理端口的情况。

Observium 是一个网络和主机监控器，它可以扫描地址范围使用通用 SNMP 登录凭证来监控系统。结合了系统和网络监控与性能趋势，它使用静态和自动发现来发现服务器和网络设备，利用各种监控方法，并可以用于配置来追踪任何可用的指标。Web UI 非常干净，并且易于使用。

Zabbix 是全面的网络和系统监控工具，它集成了多个功能到单个基于 Web 的控制台。它可以配置为监控和收集来自各种服务器和网络设备的数据，对每个对象提供服务 and 性能监控。通过广泛的工具监控服务器和网络。它的 Zabbix 代理可用于大多数操作系统，或者你可以使用被动或外部检查，包括 SNMP 到监控主机和网络设备。你还会找到大量警报和通知功能，以及高度可定制 Web 用户界面，可以适应各种显示器的高度。此外，Zabbix

具有特定工具来监测 Web 应用程序堆栈和虚拟化管理程序。

Ntop (现在的“下一代”被称为 Ntopng) 是数据包嗅探工具, 其 Web 用户界面显示网络流量的实时数据。它使用 C 语言编写, 完全独立, 可以帮助你监控网络流量, 并连接到快速简单的 Web 图形用户界面。你运行配置为观察特定网络接口的单个程序, 就可以监控了。网络流量的实时数据可以在高级实时图形功能中查看。主机数据流和主机通信对信息同样也可以实时查看。

网络运维统一平台建设方案

根据学校的网络运维的实际需求和开源工具的比较选择平台建设方案如下。

采用 LAMP 网站架构方案

LAMP (Linux- Apache-MySQL-PHP) 网站架构是目前国际流行的 Web 框架, 该框架包括: Linux 操作系统, Apache 网络服务器, MySQL 数据库, Perl、PHP 或者 Python 编程语言, 所有组成产品均是开源软件, 是国际上成熟的架构框架, 很多流行的商业应用都是采取这个架构, 和 Java/J2EE 架构相比, LAMP 具有 Web 资源丰富、轻量、快速开发等特点, 微软的 .NET 架构相比, LAMP 具有通用、跨平台、高性能、低价格的优势, 因此 LAMP 无论是性能、质量还是价格都是企业搭建网站

的首选平台。

以 Cacti 为基础平台, 整合其他开源工具和插件。

通过安装 Npc 插件整合 Icin、ga, 并按需安装 Weathermap、Monitor、Threshold、Syslog 等插件, 以实现网络设备、链路流量、服务器状态、应用状态等等的实时图形化监控和异常触发邮件报警以及日志收集分析。

整合用户网络报障处理、故障处理流程跟踪、知识库管理功能

利用开源的系统, 整合定制成符合我校需求的网络服务平台, 包括用户故障报修、故障工单指派、处理进度跟进、处理结果确认、故障处理知识归档等等。

其他功能模块

比如可以通过 PHP 的 socket 网络编程把 telnet 命令编写到网页程序中, 并根据不同类型设备定制相应的登录脚本, 实现通过执行相应的命令对网络设备进行根据权限修改配置、定时批量备份配置文件等等常用的网络运维操作, 并可针对不同级别用户授予不同的执行命令的权限。

亦可以整合 dhcpstatus 开源软件, 通过 Web 页面展示出来, 并设置阈值进行预警。



治安监控综合实施方案

山东 徐源培 崔冬梅

项目背景

治安监控项目作为一项民心工程, 在保障人民群众生命财产安全, 威慑犯罪份子方面发挥着积极而重要的作用。广电作为准运营商, 拥有覆盖广泛的光缆资源以及成熟的技术方案, 为该项目的顺利实施提供了有力的保障。该项目二期计划安装摄像头 170 余个, 并依托摄像头厂商网管系统建立监控平台, 融合一期 40 余路摄像头, 进一步实现监控的全覆盖无缝隙。

项目实施方案

根据该治安监控项目的综合需求和监控地点的实际情况, 加之设备能够方便取电, 同时兼顾设备以及后期网络的运行稳定, 我们计划使用 EPON 设备来实施。EPON 设备在业内拥有良好且成熟的使用背景, 以及设备运行可靠稳定、方便维护、可远程管理等优点。故可直接采用摄像头连至 ONU, 然后 ONU 上联至 OLT, 数据经 OLT 汇聚后通过光缆传输至派出所 H3C 交换机。

项目实施规划

VLAN 规划

该项目计划使用 VLAN 286，在 OLT、交换机和 ONU 上透传，VLAN 网关设置在派出所交换机上。

IP 规划

计划使用 38.56.27.0/24 网段作为此项目二期监控摄像头和网络设备 IP 地址，37.56.26.0/24 作为一期摄像头和网络设备使用。

EPON 配置

为保证利用 EPON 设备开展业务安全，我们将关闭 ONU 自动认证功能，严格对上线 ONU 进行手动 MAC 认证，为方便后期设备管理我们又定义了 ONU 设备网管 IP。为充分保障设备带宽和查看视频的流畅，我们将使用链路聚合方式进行数据传输。链路聚合意思是将物理上的多个端口捆绑到一起形成一个逻辑上的端口，在增加设备传输带宽、流量负载分担以及链路备份方面发挥着积极的作用，后期随着流量的增加我们可以方便进行扩容，接下来我们先进行 OLT 的配置。

OLT 和交换机链路聚合配置

首先我们配置 H3C 交换机的链路聚合，配置命令即：

```
sys
// 进入配置模式
vlan 286
// 创建 VLAN
interface Eth-Trunk 1
// 创建链路聚合组
description TWHUIJU
// 添加描述
port link-type trunk
// 定义链路聚合组端口模式
port trunk allow-pass vlan 286
// 定义端口允许通过的 VLAN
interface Gigabit Ethernet 0/0/24
// 进入端口
duplex full
// 端口全双工
speed 1000
// 端口千兆
eth-trunk 1
```

```
// 将端口加入链路聚合组
interface Gigabit Ethernet 0/0/23
// 进入端口
duplex full
// 端口全双工
speed 1000
// 端口千兆
eth-trunk 1
// 将端口加入链路聚合组
```

上面我们完成了 H3C 交换机的链路聚合组配置，接下来我们再配置 OLT 设备，配置命令如下：

```
trunk group 2 1, 5
// 创建链路聚合组并加入端口
Interface range 1, 5
// 进入端口
description H3CTW
// 添加端口描述
switchport mode trunk
// 定义端口模式
switchport trunk allo wed vlan 286
// 定义端口允许通过的 VLAN
speed 1000
// 端口千兆
duplex full
// 端口全双工
OLT 设备配置
config
进入配置模式
create vlan 77, 286 active
```

```
// 定义 ONU 网管 VLAN77 摄像头业务传输
VLAN286
interface range port 2-7
// 进入 PON 口
description TW
// 对 PON 口进行描述
switchport trunk allo wed vlan 77, 286
// 透传 VLAN 77 和 286
switchport mode trunk
authentication mode none
// 定义 ONU 的认证模式无，即自动创建和上线
ONU 配置
fttx
```

```
// 进入配置模式
interface onu 6/7/8
// 进入 ONU
uni range ethernet 1-4
// 进入端口 1 到 4
vlan mode tagged
// 定义端口模式
native vlan 286
// 定义端口 VLAN
```

上边命令对某一个上线的 ONU 进行了配置, 其他上线的 ONU 可以进行相同的配置。考虑到未来可能会将数据传送至指挥中心, 并实现与其他派出所互联, 后期再通过路由模式进行传输时, 只需新加透传的互联 vlan 即可。

后期维护

ONU 接收光功率建议在 -10dB~-22dB 之间, 工程完工后计划使用 “what’s up gold” 画出所有 ONU 的拓扑图便于网管, 同时也可结合瑞斯康达网管软件本身的网管

功能进行网管。

在设备的后期网络维护过程中可以远程使用一些 show 命令查询设备各项指标, 及时的发现问题, 快速锁定故障点简化设备维护难度。如 show interface onu online-information 和 show interface onu creation-information 查看 ONU 的在线信息和创建信息; show mac-address-table l2-address vlan 286 查看 vlan286 的 mac 地址, 即摄像头和视频服务器的 mac 地址, 方便了我们查看设备的在线个数和其他情况; 还有就是在 ftx 模式下使用命令 show interface onu 6/7/8 transceiver detail 查看 6/7/8 ONU 的光功率; 使用命令 trace mac-address 6CE5.BB5E.B8D9 (MAC 地址一定要大写) 可以查看摄像头 MAC 地址的路径。

本项工程是当地广电承接的首例天网工程, 只有科学的设计、合理的施工以及后期及时的维护才有可能打造出一个优质的视频监控工程, 从而最大限度发挥维护社会治安的作用。本项天网工程成功的实施, 不仅会为我们开展增值业务积累经验, 同时增强了与当地其他电信运营商竞争的筹码, 从而为下一步开展更多的增值业务打下良好的基础。

利用工具建立监控模型

福建 王刚 郑洪飞 荣世辉

一般网络流量监控使用的方法和技术

监控网络流量主要有基于流量镜像协议分析技术、基于硬件探针技术、基于 SNMP 的流量监测技术和基于 NetFlow 的流量监测技术。

基于流量镜像协议分析技术。流量镜像协议分析一般是把需要监控的交换机或路由器的某一个端口给分析协议或设备, 而这个端口是镜像了此交换机或路由器的所有端口的流量, 即相当于把需要监控的端口流量也复制一份给此连接分析协议或设备的端口, 此方法的优点是网络结构简单, 缺点是此方式一般针对单个端口和链路, 对交换机或路由器要求较高, 长时间会给交换机或路由器造成较大压力。

基于硬件探针的监测技术。该技术主要是在网络线路上获得数据报文, 用探针设备处理分析后得到关于网络流量的各种信息。方法是把硬件探针设备串联到串接在待监测的链路上, 对链路上的报文进行提取和分析, 将提取到流量数据进行采集和记录, 然后发送到后台数据库, 其优点是能够对高速端口的流量进行采集, 不影响原有设备的传输和性能, 不需要交换机和路由器参与工作, 流量统计较为精确, 安装相对简单, 缺点是一个硬件探针同时只能监测一条或几条链路的流量信息。

基于 SNMP 的流量监测技术。SNMP 即简单网络管理协议, 这种技术本质上是使用监测设备提取网络设备本身提供的 MIB (管理对象信息库) 来获取网络流量的

一种技术。优点是可以提供较长时间的数据监测，缺点是功能相对简单，获取的信息量有限，流量监测存在一定的误差。

基于 NetFlow 的流量监测技术。NetFlow 流量统计技术是思科公司提出，目前已经成为一种网络流量统计标准。共有 5 个版本，其中版本 5 为目前主流使用版本。其本质是将流量数据的协议、流量、端口、硬件地址、IP 地址、服务类型等信息保存在 NetFlow 缓存中，然后被发送到后台的流量采集设备或服务器进行处理，目前，很多电信企业将之作为一种计费管理技术使用。优点是实时性好，配置方便简单，可在高速链路上使用，监控的数据精确，缺点是价格较高。

Sniffer Pro 的一些特点

Sniffer Pro 是著名网络协议分析软件，是最常用的抓包分析软件之一，广泛应用于网络故障分析、流量分析、协议分析、网络安全检查、非法设备接入检查、网络攻防等方面，不需要额外的硬件支持。可以对监测各条链路流量、阻塞、业务等，可提供包括网络统计信息、应用层统计信息、告警和通知、实时解码、实时专家分析在内的实时数据或图表方式显示监控结果。

Sniffer Pro 监控网络流量模型

网络拓扑

使用 VMware 分别模拟各个服务器和计算机，其模拟环境如图 1 所示。

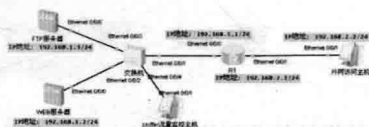


图 1 模拟环境拓扑

统计内容

流量类型、当前网络每秒收 / 发数据包速度、收集所有节点信息，提供每个节点相应统计结果、统计网络中所有主机的会话列表、统计应用层协议的响应时间、对全网网络规模和利用率分布做统计。

统计流程

一是利用 VMware 分别模拟各个服务器和计算机，并按模拟环境设置相应 IP 地址。在 FTP 服务器上使用“守望 FTP 服务器”架设 FTP 服务器，在 Web 服务器上使用“简易 http 服务器”架设 Web 服务器。如图 2 所示。

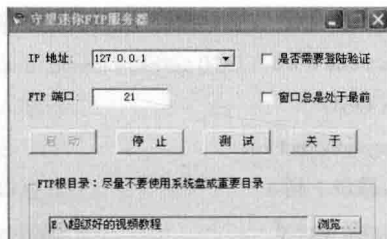


图 2 架设 FTP 服务器

二是给路由器 Ethernet 0/0/0 和 Ethernet0/0/1 分别设置 IP 地址作为网关，确保外网访问主机可以 Ping 通内网 FTP 服务器和 Web 服务器。如图 3 所示。

```
interface Ethernet0/0/0
ip address 192.168.1.1 255.255.255.0
#
interface Ethernet0/0/1
ip address 192.168.2.1 255.255.255.0
#
```

图 3 路由设置 IP 地址

三是在交换机上将 Ethernet0/0/1 数据镜像至 Ethernet0/0/4。如图 4、图 5 所示。

```
#
observe-port 1 interface Ethernet0/0/1
#
```

图 4 设置交换机 Ethernet0/0/1 为被监控端口

```
interface Ethernet0/0/4
port-mirroring to observe-port 1 inbound
port-mirroring to observe-port 1 outbound
```

图 5 设置交换机 Ethernet0/0/4 为监听端口

四是使用外网访问主机访问内网 Web 服务器和 FTP 服务器（可以下载 FTP 内的相关资料），如图 6 所示。



图 6 使用外网访问主机访问内网 Web 服务器

五是利用 Sniffer 进行分析。分别利用仪表板、主机列表、矩阵、请求响应时间、历史取样、全局统计表达和协议分布的相关信息，如图 7 所示。



图 7 利用 Sniffer 分析取样和监控网络流量

❖ 日志审计分析系统的应用

▼ 武汉 李懿

数据中心作为企业信息化建设中的核心，由大量网络设备、安全设备、操作系统、应用服务等组成，管理员要对所管理的各种设备进行巡检，以及时发现问题，但面对海量的日志数据，如何进行有效处理，成为管理员所面对的问题。

日志审计分析系统（下简称日志系统）作为统一的日志收集与分析平台，在数据中心的作用既有日常管理作用，也有安全审计作用。日志系统通过对数据中心网络设备、安全设备、服务器、应用系统日志进行全面的标准化收集和存储，为管理员提供了集中的日志查看、检查平台，通过日志系统的关联、分析、告警功能，帮助管理员第一时间了解各类安全事件，通过各类报表、查询功能，为管理员提供合乎法规、内控要求的报表。

日志系统可以方便的部署到现有数据中心网络环境中，只要网络能够到达平台即可实现日志的收集，但由于需要获取相关网络流量日志，建议一般连接在核心交换机上。

日志系统日志采集方式主要有安装代理方式，主要在操作系统内安装代理程序，与管理平台相关联，将系统日志发送给管理平台。

syslog 方式，适用于网络设备及安全设备，在设备中启用 syslog 进程，将管理平台地址设置为日志发送地址；端口镜像方式，在网络设备配置流量镜像端口，与管理平台相连，在管理平台上进行端口过滤，得到诸如数据库、web 访问等的流量数据，从而形成相应日志信息；文件采集方式，可定时将文本型日志采集到管理平台进行存储分析。

日志系统在对海量日志收集后，用户需要平台自带的关联分析功能、规则定义功能、日志报表的定义，来实现管理员对日志分析的要求。以下从几个不同日志类型来了解。

1. 数据库日志

一般来说有两种，一种是通过字段收集直接发送给日志系统，另一种日志系统通过流量端口过滤主动抓取。不管是哪种收集日志方式，日志系统通过自身的关联分析引擎，能够产生一段时间内用户对数据库操作的语句记录，或者产生一段时间内用户登录数据库的登陆记录，管理员通过查看这些信息检查数据库是否存在健康或安全问题，如图 1 所示。

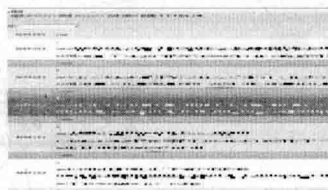


图 1 数据库操作记录

2. 操作系统日志

一般来说，通过在操作系统内安装代理程序，将操作系统产生的事件日志直接发送给管理平台。这种日志首先需要管理员在操作系统中进行启用配置，默认情况下，Windows 操作系统安全策略审核日志是不开启的，需要手工配置，以保证所需要的日志能产生，其次需要管理员明确所关注的事件及相应事件项，比如系统的开关机、登陆的成功或失败、磁盘问题等，这些在日志系统中基本都有内置规则，管理员也可根据自己需求自定义规则，如图 2 和图 3 所示。

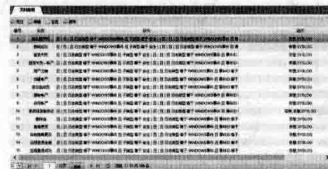


图 2 审核日志



图 3 定义日志规则

3. 网络及安全设备日志

此类日志是通过启用 syslog 进程，将设备日志发送到日志系统。

对此类设备，管理员通常会关心设备状态、性能等，那么对于该类日志分析，建议管理员收集日志关键字，自定义或使用内置报表，生成报表后供管理员使用，如

图 4 所示。

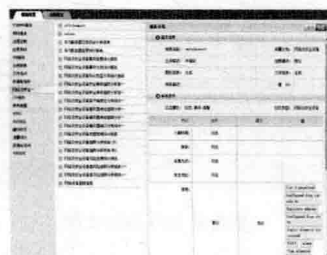


图 4 关心设备状态性能

上述三种类型的日志为比较常用的日志，涉及到了日志平台的关联引擎、内置规则、报表定义等方式。

管理员在使用时可以灵活使用，还可以利用日志系统短信、邮件功能发送所关注的日志，使管理员能利用日志平台及时了解数据中心内系统、应用状态，提高对数据中心服务故障的响应。

利用端口聚合增加交换网带宽

甘肃 左振辉

如图 1 所示，sw1 为核心交换机，连接汇聚层设备、内网服务器和英特网，sw2 为汇聚层交换机，连接核心层设备和接入层交换机，sw1 和 sw2 之间的链路常常成为网络瓶颈。

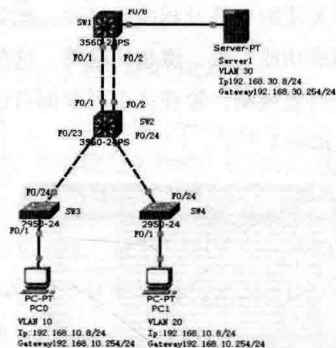


图 1 交换型网络拓扑结构

端口聚合

逻辑端口 AP (Aggregate Port) 由多个物理成员端口聚合而成，是链路带宽扩展的重要途径，其标准为 IEEE802.3ad。此外，通过聚合端口发送的帧还可以在所有成员端口上进行流量平衡，如果 AP 中的一条成员链路失效，聚合端口会自动将这条链路上的流量转移到其它有效成员链路上提高连接的可靠性。这就是 IEEE802.3ad 所具有的自动链路冗余备份功能。当交换机得知 MAC 地址已经被自动地从一个 AP 端口重新分配到同一链路中的另一端口时，流量转移就被触发，数据将通过新端口转发，这一过程在数毫秒内完成，几乎不影响网络服务。聚合端口 AP 中任意一条成员链路收到的广播或者多播报文，不会被转发到其他成员链路上。同一个 AP 的成员端口必须为同类型，全是 Access 模式或 Trunk 模式。

流量平衡

AP 将根据报文的源 MAC 地址、目的 MAC 地址或者源 IP 地址、目的 IP 地址进行流量平衡，把流量均衡的分配到 AP 的成员链路中去。依据源 MAC 地址或目的 MAC 进行流量平衡时，不同主机或目的主机的报文转发的链路不同，同一台主机或目的主机的报文，从同一条链路转发。依据源 MAC+ 目的 MAC 地址进行流量平衡时，有不同的源 MAC+ 目的 MAC 地址的报文，可能被分配到同一个 AP 成员链路中。

依据源 IP 地址或者目的 IP 地址，以及源 IP 地址 + 目的 IP 地址进行流量平衡时，不同的源 IP 地址或者目的 IP 地址的报文通过不同的端口转发，同一源 IP 地址或者目的 IP 地址的报文通过相同的链路转发。该流量平衡方式一般用于三层交换机的聚合端口。在此流量平衡模式下，如果收到的是二层报文，则自动根据源 MAC 地址、目的 MAC 地址进行流量平衡。根据不同的网络拓扑结构设置合适的流量平衡方式，以便能把流量较均衡地分配到各个链路，就可以充分利用网络带宽，提高网络效率和稳定性。

服务器上使用随身 WiFi

湖南 曹彩武

随身 WiFi 方便，不受网线的约束，可以随时随地上网。但这仅限于在 Windows XP 或 Windows 7 或最新 Windows10 等操作系统上实现。随身 WiFi 如果接在 Windows Server 2003 或者 Windows Server 2008 等操作系统上，驱动程序是装不上去的。

那么，如何让随身 WiFi 能在 Windows Server 服务器操作系统上运行呢？

1. 把随身 WiFi 连接 USB 口，系统会提示你安装驱动程序。如果你用随身 WiFi 自带的光盘或者去官网下载相关驱动，安装时会提示此驱动不适用于该操作系统，如图 1 所示。

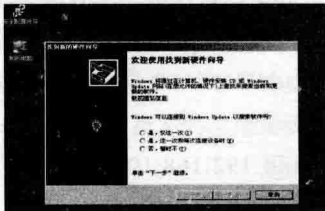


图 1 安装驱动程序窗口

2. 在互联网下载 Ralink 雷凌 RT2870USB 无线网卡驱动 5.1.5.0 版驱动或者直接用 360 驱动大师等其它软件将随身 WiFi 驱动为无线网卡，安装后大家右击 - 网上邻居 - 属性可以看到一个“无线网络连接”图标，则证明无线

网卡驱动成功。建议用后一种方法安装驱动程序，如图 2 所示。

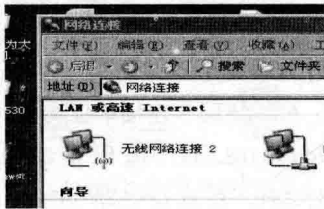


图 2 网络连接窗口

3. 安装模拟 WiFi 热点的软件，有一些 WiFi 热点软件在 Windows Server 下不能用，但笔者确认 WiFi 共享精灵和 160WiFi 可以，当然大家也可通过互联网搜索相关的 WiFi 软件，安装试用后找到合适的，图 3 是笔者所用的，分别设置 WiFi 名称和密码即可。



图 3 模拟热点窗口

4. 右击 - 网上邻居 - 属性 - 无线网络连接 - 设置 IP

地址,如图4所示。



图4 设置IP地址窗口

按照上述方法设置后,大家可以尝试用手机等设备搜索 WiFi 热点,是不是成功了呀?

看到这里,大家可以考虑一下,如果你有一台笔记本,而笔记本电脑又带有无线网卡。那么你是不是不用购买随身 WiFi 就可以把笔记本电脑变身为无线路由器了呢?答案是肯定的。

双网卡同时访问的设置方式

山东 任志强

作为网络维护人员有时会遇到同一台 PC 或服务器有两块网卡,既要访问局域网内各网段又要访问公网。当然,最简单的方式是访问公网时将内网网卡禁用,用公网的网卡访问公网,访问内网时将公网网卡禁用,再启用内网网卡。但操作起来较繁琐,下面向大家介绍有一种方法简单实用的方法。

现有一台 PC 其中一块网卡通过傻瓜式路由器直接连接公网,另一块网卡连接单位局域网,分配的静态 IP 地址为 182.168.5.11,掩码是 255.255.255.0,网关是 182.168.5.254,首选 DNS 是 192.168.3.1,备用是 192.168.3.2,内网服务器 IP 地址段为 192.168.3.0/24,还要访问 192.168.5.0/24 和 192.168.10.0/24 网段。

要求该 PC 可以双网并用,既可以上公网又可以访问内网指定网段。若要实现上述功能可用如下方式。

1. 配置访问公网的网卡,由于访问公网的网卡直接通过傻瓜式路由器连接,可以采用自动获取 IP 的方式实现,如图1所示,配置完毕后点击确定。

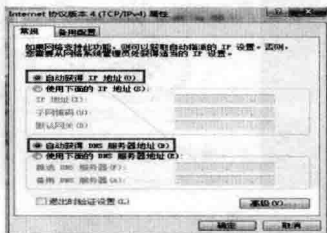


图1 配置访问公网网卡

2. 配置访问内网网卡,如图2所示(网关不填),配置完毕后点确定。

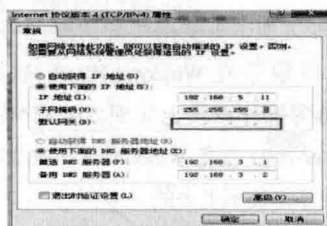


图2 配置访问内网网卡

3. 在 PC 上点击“运行”窗口中输入 CMD 进入 DOS 环境下配置如下命令:

```
Route -p add 182.168.5.0 mask 255.255.255.0 182.168.5.254
```

```
Route -p add 192.168.3.0 mask 255.255.255.0 182.168.5.254
```

```
Route -p add 192.168.5.0 mask 255.255.255.0 182.168.5.254
```

```
Route -p add 192.168.10.0 mask 255.255.255.0 182.168.5.254
```

经过上述配置即可实现双网卡同时访问,其中 -p 表示永久添加,否则重启后该条路由不被保存。add 182.168.5.0 表示添加该网段,mask 255.255.255.0 表示该网段的子网掩码,182.168.5.254 表示访问其他网段的路由均经过该网关。

如果还需要访问其他网段照此继续添加即可。

❖ 网络虚拟化技术的应用研究

▼ 新疆 陈超

技术概况

网络虚拟化是一个过程，同时也是一系列技术的统称，主要包括三方面，一是物理主机内部网络虚拟化；二是对网络交换设备的虚拟化；三是对网络虚拟化的统一管理。

在一套物理网络上采用虚拟技术划分出多个虚拟交换机或多个相互隔离的逻辑网络，是 1:N 的虚拟化；将多个物理网络设备虚拟整合成一台逻辑设备或多条物理链路聚合成一条逻辑链路，简化网络架构，是 N:1 的虚拟化。通过网络虚拟化可实现弹性、安全、自适应、易管理的基础网络，充分满足服务器虚拟化等虚拟技术对基础网络的要求，达到提高虚拟服务器效率的目的。

网络虚拟化在吐哈信息网的应用

吐哈信息网经过几年的建设和完善，已经形成了鄯哈双核心、核心至汇聚双链路的网络结构，还建成了哈密数据中心、鄯善数据容灾中心、财务专网、视频会议专网、视频监控专网等，广泛采用了网络虚拟化的早期技术 VLAN、LAG、OSPF，信息网络基础架构不断完善。网络虚拟化技术应用情况如下。

1.VLAN 应用

社区网 10.80.0.0 网段在用子网段 300 个，企业网 10.218.0.0 网段在用子网段 339 个，基本上是一个子网段对应一个 VLAN。VLAN 技术的应用增强了网络的安全性、灵活性。

2. 应用 VRRP 虚拟路由冗余协议

使社区网 H3C S8508、H3C S9508E 实现双核心双机主备，当双核心设备一台出现故障时，可以及时的由另一台设备来代替，实现双核心之间、核心到汇聚交换机之间数据的自动迁移，使双核心交换机通过主备模式实现双机热备和冗余。从而保证了社区核心网络的连续性和可靠性，如图 1 所示。

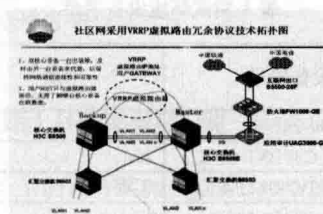


图 1 社区网 VRRP 技术应用拓补

3.OSPF 技术应用

企业网鄯哈核心互联采用了 OSPF 技术，鄯哈核心至汇聚层使用 OSPF 技术实施双链路双路由 26 对。使用 OSPF 技术，双链路之间切换时间为 10-30 秒，为网络接入业务提供了较为可靠的链路容灾保障。如图 2 所示。

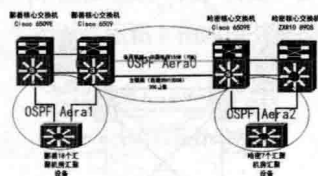


图 2 企业网 OSPF 技术应用拓补

IRF 网络虚拟化技术的应用研究

1. 原理介绍

IRF（Intelligent Resilient Framework，即智能弹性架构），它是 H3C 专有的设备虚拟化技术，它同样可将实际物理设备虚拟化为逻辑设备供用户使用。IRF 形成的虚拟设备采用 1:N 冗余，即 Master 负责处理业务，Slave 作为 Master 的备份，随时与 Master 保持同步。当 Master 工作异常时，IRF 将选择其中一台 Slave 成为新的 Master，由于在 IRF 系统运行过程中进行了严格的配置同步和数据同步，因此新 Master 能接替原 Master 继续管理和运营 IRF 系统，不会对原有网络功能和业务造成影响，同时，由于有多个 Slave 设备存在，因此可以进一步提高系统的可靠性，原理图如图 3 所示。

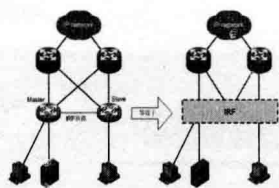


图3 原理图

2. 应用可行性研究—IRF

(1) 测试环境设备清单：如表1所示。

表1 测试环境设备清单

编号	设备型号	用途	数量
1	H3C S5500-28F-EI	核心	1
2	Cisco WS-C3750G-48TS	核心	1
3	H3C S3600V2-52TP-EI	汇聚	2
4	Cisco WS-C2960-48TC-L	接入	1
5	便携式 PC	NTP 服务器及测试	1

(2) 测试环境网络架构拓扑：模拟企业网哈密核心汇聚接入三层架构，双核心双链路聚合并采用 OSPF 协议互联。双汇聚通过 IRF 配置命令 `ief number 1 rename` 将两台设备虚拟成一台设备，虚拟设备通过跨设备端口聚合分别与双核心双链路采用 OSPF 协议互联，虚拟设备通过跨设备端口聚合与接入层双链路采用二层 TRUNK 技术互联。网络拓扑图如图4所示。

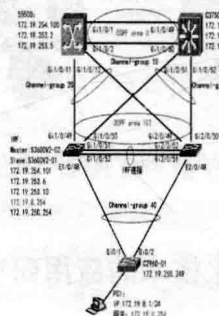


图4 网络拓扑结构

(3) 测试项目

测试一：断开 IRF 系统 master 设备 S3600V2-02 电源。IRF 系统的 master 离开后，IRF 系统会重新选举 master，并重新计算拓扑。IRF 系统 master 设备 S3600V2-02 断电后，ping 业务网关 172.19.8.254 未丢包，ping 核心 S5500 接口地址 172.19.253.5 未丢包，ping 核心 C3750G 接口地址 172.19.253.9 未丢包。查看 IRF 系统日志，18:03:17:190 时发现堆叠口状态变化，18:03:18:066 时完成拓扑计算，时间间隔是 876 毫秒。

测试二：恢复 IRF 系统 master 设备 S3600V2-02 供电。IRF 系统新成员加入后，IRF 系统会重新选举 master，并

重新计算拓扑。IRF 系统 master 设备 S3600V2-02 供电恢复后，ping 业务网关 172.19.8.254 未丢包，ping 核心 S5500 接口地址 172.19.253.5 未丢包，ping 核心 C3750G 接口地址 172.19.253.9 未丢包。查看 IRF 系统日志，18:07:50:437 时发现堆叠口状态变化，18:07:51:079 时完成拓扑计算，时间间隔是 642 毫秒。

(4) 测试结果分析

采用 IRF 堆叠技术将两台汇聚设备虚拟为一台设备，汇聚层与核心层、汇聚层与接入层都采用了跨汇聚设备端口聚合技术。汇聚层与核心层还应用了 OSPF 技术，IRF 系统中一台设备故障后，另一台设备仍然担负着数据转发，因此不会造成接入业务的网络中断，IRF 网络虚拟化技术应用可行。

3. 油田公司视频会议系统 IRF 应用建议方案

鄯哈视频会议系统分别部署两台 H3C S5500-28-EI 作为汇聚交换机，鄯善学术报告厅五号会议室、哈密机关二楼机房、哈密副楼三楼机房分别部署 2 台 S3600V2 作为接入。使用 IR 网络虚拟化技术 F 对鄯善 2 台视频会议汇聚交换机进行虚拟化叠加，对哈密 2 台视频会议汇聚交换机进行虚拟化叠加，分别对每个会场的 2 台接入交换机进行虚拟化叠加。鄯哈汇聚层双链路采用 OSPF 协议互联，汇聚层至接入层双链路跨设备端口聚合并采用二层 TRUNK 技术互联，消除了汇聚层及接入层的单点故障，如图5所示。

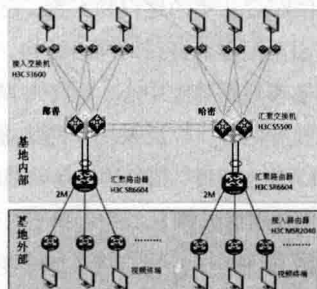


图5 油田公司视频拓扑

结语

网络虚拟化是将多个硬件或软件网络资源及相关的网络功能集成到一个可用的软件中统一管理和控制的过程。随着各项业务对网络的依赖度逐渐加大，业务对网络基础架构的稳定性要求也越来越高，核心、汇聚、接入三层设备和链路热备或负载分担将成为网络架构的主流，在今后网络建设中，我们要根据实际需要灵活运用各种网络虚拟化技术来组建网络，确保网络的稳定性。

❖ 端口隔离在网络管理中的应用

▼ 深圳 李逸飞 李发成

作为一个网络管理者，需对联网计算机采取隔离措施。以下是我在单位中常遇到需要隔离的事例。

事例 1：要在电脑教室中进行某类考试，各计算机之间不允许互相通信。但每台学生机必须能联通到教师机，因为教师机需要给每台学生机下发试题，同时学生机需要上交试卷到教师机。

事例 2：学生喜欢联网共享游戏，这就需要学生机互相隔离。但学生机是需要联通到学校局域网和 Internet 的，因为学生需要访问学校网站和到外网上查找资料。

事例 3：根据需要进行分组隔离。

联网计算机相互隔离的方法

方法一：通过操作系统本身禁止共享和访问。

1. 在“服务”中关闭“Server”服务和“Workstation”服务；
2. 在“用户权限分配”的“允许从网络访问这台计算机”中删除“Everyone”和“Guest”等用户；
3. 在“拒绝从网络访问这台计算机”当中增加“Everyone”和“Guest”等用户。

方法二：通过 VLAN、子网或 ACL 进行隔离。

把需要隔离的计算机划分到不同的 VLAN 中；或把需要隔离的计算机划分到不同的子网中；或利用 ACL 等。这些都可以实现隔离的目的，但都没有端口隔离来得简明扼要。

方法三：通过交换机的端口隔离进行隔离。

不同型号交换机的端口隔离命令有些区别，比如有些 Cisco 和锐捷交换机隔离命令是 switchport protected。有些华为和 H3C 交换机隔离命令是 port-isolate enable 或者 port isolate；有些神州数码交换机隔离命令是 isolate-port allowed ethernet <InterfaceList>。本文以华为 S5700

为例，其他型号可举一反三。

单交换机端口隔离的实现

如图 1 所示的拓扑结构，g0/0/1-g0/0/22 为学生机端口，g0/0/23 为教师机端口，g0/0/24 为上联端口。其中上联端口和教师机端口不要被隔离，只把学生机所在的端口隔即可。隔离命令为：

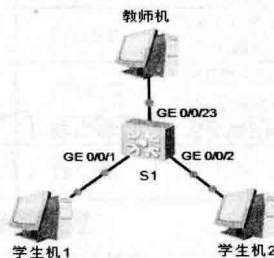


图 1 单交换机拓扑结构图

```
interface g0/0/1 to g0/0/22
port-isolate enable
```

跨交换机端口隔离的实现

事实上，如果电脑室有 56 台计算机，若使用 24 电口交换机就需要三台。通过实际操作会发现下面的问题，计算机接入端口被隔离后，同一交换机下的所有计算机确实是被隔离了，但跨交换机之间的计算机仍然是能 ping 通的。也就是说，计算机所在端口隔离只隔离了同一交换机端口下的计算机，对于跨交换机端口下的计算机并没有被隔离。如图 2 所示的跨交换机拓扑结构图中，学生机 1 和学生机 2 被隔离了，但学生机 1 和学生机 3、学生机 1 和学生机 4 还是可以通信的。

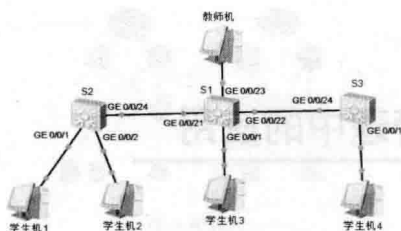


图 2 跨交换机拓扑结构图

要实现跨交换机的隔离，必须要把承担着汇聚的交换机 S1 的下联端口当成普通接入端口进行隔离，如图 2 所示的拓扑图中 S1 的 GE0/0/21 和 GE0/0/22 端口。而各交换机的上联端口是不能被隔离的，如 S1、S2 和 S3 的 GE0/0/24 端口，否则上联端口不能转发数据。S1 具体配置如下：

```
interface range GE0/0/1 to GE0/0/22
```

```
port-isolate enable
```

S2 和 S3 的配置同理可得，略。

分组隔离

如图 3 拓扑图所示，假如学生机 1、学生机 2 为第

一隔离组，学生机 3、学生机 4 为第二隔离组。配置命令如下：

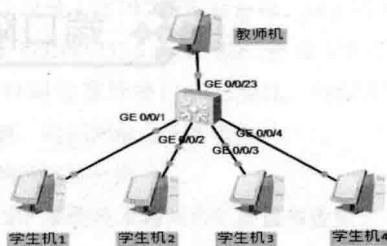


图 3 分组拓扑结构图

```
[S1]port-group 1
```

```
[S1-port-group-1]group-member g0/0/1 to g0/0/2
```

```
[S1-port-group-1]port-isolate enable group 1
```

```
!
```

```
[S1]port-group 2
```

```
[S1-port-group-1]group-member g0/0/3 to g0/0/4
```

```
[S1-port-group-1]port-isolate enable group 2
```

国际 EPC 项目的网络规划

▼ 辽宁 王一军

项目背景

某国际 EPC 项目（E 设计、P 采购、C 施工）建设规模为 $1 \times 344.908\text{MW}$ （净）燃气-蒸汽联合循环发电机组。与笔者所在公司以往项目中所承担的 C 角色（施工承包方）不同，按照 EPC 合同规定，作为 EPC 承包商，不仅对外需要为业主及业主咨询公司提供网络，同时对内需要给设备、设计、运输、调试、运维等分包商提供网络支持。

随着服务对象的扩大，在网络规划、网络安全等方面提出了新的管理课题。同时，项目部既主要应用于日常办公，提高沟通效率，又要考虑方便职工在业余时间

与国内联系，提供感情沟通、情绪排解的渠道。所以，在网络规划时，要同时考虑办公区应用与生活区应用两部分。

总体设想与规划方案

1. 总体设想

采用“一网两隔离双分开”方法。即整个现场使用一条外线进线，但内部局域网络中，EPC 团队（含笔者所在公司，以及在现场的设计、运输、设备厂家、调试、运维、施工分包单位）与外方业主与咨询公司网络隔离；在 EPC 内部，办公应用与生活区应用分开。

2. 规划方案

- (1) 逻辑方面：外方业主（含咨询公司）与 EPC 团队使用不同网段。EPC 团队使用笔者所在公司总部统一分配的 VPN 网段，而外方业主使用通用的 192 网段，确保两个网段无法相互访问。
- (2) 硬件方面：EPC 团队与外方业主网络接入到同一个路由器上不同的 LAN 接口，确保相互隔离。
- (3) 办公区网络环境方面：所有办公场所考虑有线接入，根据人员配置情况，每个房间分配 4 条网线（EPC 团队办公区）或者 2 条网线（业主办公区），每台电脑采用固定 IP 地址，并与 MAC 地址绑定。
- (4) 生活区网络环境方面：生活区宿舍接入 WiFi 无线网络，各种移动设备随机动态分配 IP 地址。

3. 生活区网络规划

根据项目部要求无线网络覆盖整个生活区的总体部署，考虑在生活区每栋宿舍都投入 1 至 2 个无线路由；同时根据整个 EPC 团队人数策划，项目高峰期时国人数量在 350 人以上。

考虑大部分职工都同时使用笔记本、智能手机或者 PAD 上网的情况，预计人数高峰期间时网络接入点总体量要超过 500 点左右，而一个常规网段最大支持 254 个接入点，故采用划区划域、组建生活区若干 WiFi 子网的规划方案。

根据生活区宿舍的实际布局和房间人数分配的原则，将生活区无线网络划分成几个区域，将每个区域的某一台无线路由的 WAN 口直接接入到项目部机房交换机上，分配一个项目部内部 IP 作为“外网”地址。

该区域的其他无线路由接入到该无线路由的 LAN 口上，可同时接入 4 个无线路由，再分配各个路由对应的动态 DHCP 地址范围；这样，整个生活区接入容量可实现约 N*254 的体量，N 为生活区子网数量。

网络配置与网络参数设置

1. 网络拓扑结构

网络拓扑图见图 1 所示。其实现方法为：在接入一条外线的情况下，项目部内网接入到总路由器的 LAN 口，业主网络接入到总路由器的 LAN1 口，确保物理上的隔离。

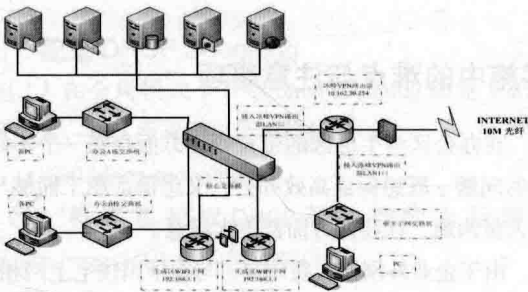


图 1 网络拓扑图

2. 网络设施配置

外部网络的情况是：光纤接入，固定外部 IP，10M 带宽；网络设备相关信息如表 1 所示。

表 1 网络设备信息

序号	设备用品	设备品名	功能与参数配置	规格型号
1	总路由器	冰峰 (IECFLOW)	企业级 VPN 路由器	Enterprise 5210
2	生活区路由器	TPLINK	750M 双频千兆无线路由器	TL-WDR4320
3	生活区路由器	TPLINK	1.75G11AC 双频千兆无线路由器	TL-WDR7500
4	交换机	D-LINK	二层构架，48 口	DES-1048
5	交换机	TPLINK	二层构架，24 口	DES-1024A

3. 网络参数设置

EPC 团队办公区与外方业主办公区网段分配如表 2 所示。

表 2 团队与业主办公区网段分配

区域	EPC 团队办公区	外方业主办公区
网段	10.162.30.X	192.168.1.X
掩码	255.255.255.0	255.255.255.0
网关	10.162.30.254	192.168.1.1

EPC 生活区各 WiFi 子网内接入项目部网络的无线路由 LAN 地址均为 192.168.1.1，子网内其他无线路由分别顺序编号，每个路由都采用 DHCP 动态分配，根据各宿舍人数情况分配不同的 DHCP 范围，但网关均指向 192.168.1.1，DNS 均指向外部当地 DNS。

应用历程以及实施情况

2013 年 2 月网络工程师到达现场；2013 年 5 月，EPC 团队生活区网络先期投入使用，随宿舍建设规模不断扩充；2013 年 9 月，EPC 办公区与外方业主办公区局域网络形成，正式投入使用。

该项目办公网络于 2013 年 9 月份全面投入使用后，

目前已经运行3年,总体上运行状态稳定,各方反映良好。

实施中的难点与注意事项

在办公区与生活区的带宽管理方面存在一个不好协调的问题:既想保证高效办公,又想保证职工能够与国内人员沟通,往往两方面都不太满意。

由于企业外网接入费用高,与在中国住宅上网相比,同样带宽的价格要高出若干倍,无法提供“随性”的外网带宽。因此需要在工作时间通过关闭生活区网络,全力保证办公网速。

在服务商与外部接线的管理方面,笔者一直倾向于有线光纤接入的外接方法,因为这种接法不像无线基站接入方式受外部环境干扰那么大。

其实在项目前期也是光纤接入,但由于项目部地处偏僻,光纤线路长,经常出现大风大雨以及人为破坏等外部因素导致光纤线路断掉。

因此,后来改用无线基站接入,不受地面人为因素干扰,反而比较稳定。

通过在本项目中的探索与实践,摸索出了一个适合国际 EPC 项目总包方应用网络的管理方法,可为其他国内公司从事其他海外 EPC 项目施工提供借鉴。

如何解决 IP 地址故障

山东 赵利然

笔者朋友维护的一个企业网(网络拓扑结构如图1所示),计算机终端均通过 DHCP 方式获得 IP 地址。

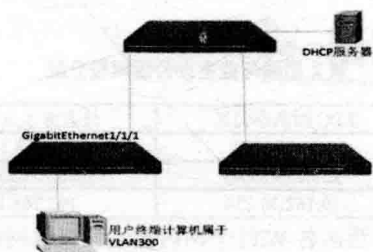


图1网络拓扑结构

最近,网内经常出现计算机终端获得其他网段地址或者因地址冲突导致不能正常上网的问题。

经调查发现,获得其他网段地址是由于网内存在私自架设的 DHCP 服务器,导致 DHCP 客户端获取错误的 IP 地址和网络配置参数;地址冲突则是因为部分计算机私自配置了静态地址造成与通过 DHCP 方式获得 IP 的计算机地址冲突。

此类问题的频繁发生,已经严重影响了正常工作。考虑到网内均采用 H3C s3600 和 s3100 交换机,因此可以综合采用 DHCP Snooping 与 ARP Detection 技术来彻

底解决这类问题。

DHCP Snooping 和 ARP Detection 技术介绍

1.DHCP Snooping

DHCP Snooping 技术是 DHCP 的安全特性,通过建立和维护 DHCP Snooping 绑定表来过滤不可信任的 DHCP 信息。具有如下功能:

(1) 保证客户端从指定的 DHCP 服务器获取 IP 地址。

DHCP Snooping 安全机制允许将端口设置为信任端口和不信任端口。

信任端口正常转发接收到的 DHCP 报文。不信任端口则在接收到 DHCP 服务器响应的 DHCP-ACK 和 DHCP-OFFER 报文后,丢弃该报文,从而屏蔽假冒的 DHCP Server。

(2) 记录 DHCP 客户端 IP 地址与 MAC 地址的对应关系。

DHCP Snooping 通过监听 DHCP-REQUEST 和信任端口收到的 DHCP-ACK 广播报文来记录 DHCP Snooping 表项,这些信息也可以作为 ARP Detection 判

断发送 ARP 报文的用户合法与否的依据之一，从而防止非法用户的 ARP 攻击。

2. ARP Detection

ARP Detection 功能主要应用于接入设备上，只有合法用户的 ARP 报文才能进行正常转发，否则直接丢弃，从而防止仿冒用户、仿冒网关的攻击。

ARP Detection 包含三个功能：用户合法性检查、ARP 报文有效性检查、ARP 报文强制转发。其中，用户合法性检查功能可以基于 DHCP Snooping 的安全表项进行，作为判断用户是否合法的依据。

3. 技术的使用

根据上述介绍，我们可以综合采用这两种技术来解决 IP 地址故障。

(1) 利用 DHCP Snooping 技术，解决 DHCP Server 私设问题。

将交换机上连接授权 DHCP 服务器的上行端口设为信任端口，保证转发接收到的正常 DHCP 报文，其他设为非信任端口。这时，非信任端口会丢弃假冒 DHCP Server 的报文，从而解决了 DHCP Server 私设的问题。

(2) 利用 ARP Detection 技术，对用户进行合法性检查，解决私配静态 IP 地址问题。

将连接授权 DHCP 服务器的上行端口设为 ARP 信任端口，此时不进行用户合法性检查。其他端口设为 ARP 非信任端口，进行用户合法性检查。由于已经启用了 DHCP Snooping 功能，因此，可以通过检查 DHCP Snooping 的安全表项，排除非法私配静态 IP 地址的用户终端，确保用户只能从指定 DHCP Server 获得地址，最终解决 IP 地址冲突问题。

具体配置方法和命令

1. 配置 DHCP Snooping

(1) 在全局模式下开启 dhcp-snooping 功能（此功能开启后，默认所有接口为不信任端口）。

```
[s3600]dhcp-snooping
```

(2) 将连接授权 DHCP 服务器的上行端口 GigabitEthernet1/1/1 设为信任端口。

```
[s3600]interface gi 1/1/1
```

```
[s3600-gigabitethernet1/1/1]dhcp-snooping trust
```

2. 配置 ARP Detection

(1) 在用户终端所属 VLAN300 启用 arp detection 功能（此功能开启后，此 VLAN 所有端口缺省为非信任状态）。

```
[s3600]vlan 300
```

```
[s3600-vlan300]arp detection enable
```

(2) 连接授权 DHCP 服务器的上行端口 GigabitEthernet1/1/1 设为信任状态。

```
[s3600-gigabitethernet1/1/1]arp detection trust
```

功能验证

网内的其他交换机也按照上述方法配置后，此时网内计算机终端只能从指定的 DHCP 服务器获取 IP 地址，不能从私自架设的伪 DHCP 服务器获取错误的 IP 地址配置信息。

用户如果私配了静态 IP 地址（即使配置了与 DHCP 服务器分配的 IP 地址一样的静态 IP 地址），也将不能正常上网，避免了地址冲突现象。

至此，通过综合采用 DHCP Snooping 和 ARP Detection 技术，所有 IP 地址问题均得到有效解决。



全网数据设备自动备份

▼ 江苏 尹德恩 王鹏 黄陆平

自动备份软件实现原理

目前，我们现网的数据设备 Cisco 路由交换、CMTS

接入设备、EPON 接入设备都有 TFTP 命令，将配置保存到 TFTP 服务器。比如：

Cisco 交换机 : copy running-config tftp。

Moto CMTS : copy running-config tftp。

EOPN 设备 : upload configuration tftp inet 192.168.10.1 configname。

都有相关的 TFTP 命令, 每种类型的设备命令格式有略微的差别。

本项目的原理就是, 将所有数据设备存放在数据库中, 并给每台数据设备定义好设备型号, PHP 程序轮询数据库, 每条记录调用 shell 脚本, 自动执行 TELNET 命令, 登录到每台数据设备, 执行下 tftp 导配置命令, 并将配置按照设备类型保存到指定文件夹。

自动备份开发要点

主要有以下几个重要项目 :

数据库

device_table 表

php 程序轮询这个表。

ip : 每台数据设备的 IP 地址, 唯一。用于 telnet 设备用。

hostname : 主机名, 通过 SNMP 获取, 用作自动备份配置时给配置起文件名。

description : 主机描述, 通过 SNMP 获取。

device_type : 设备类型, 事先定义好 (比如 : route、switch、cmts、eopn)。

model 表

model : 设备型号, 事先定义好。有两个用途 : 用于自动备份时选择 shell 脚本, 因为, 每种型号的设备 tftp 命令有区别。为每个型号做个 shell 脚本, 比较灵活, 有新型号设备, 添加一个 shell 脚本就 OK。用于给数据设备分类, 所有 TFTP 过来的配置, 都按照设备类型进行保存。

model : 数据设备录入数据库时, 提供选择, 必选。

Shell 脚本

[root@localhost shell]# ls

bsr64000.sh C4c.sh S8600.sh UBR10K4.sh
UBR7225.sh UBR7246.sh

在这个文件夹中, 存放所有设备型号的 shell 脚本, 文件名跟 model 表中的一样。

cat UBR7225.sh

#!/bin/sh

#cisco ubr7225

ip=\$1 // 由 PHP 函数传参进来, 用于 telnet 到那台设备

hostname=\$2 // 由 PHP 函数传参进来, 定义配置文件名

```
(
echo "enable";
echo *****;
echo "copy running-config tftp";
echo "192.168.10.1";
echo $hostname;
echo "exit";
)| telnet $ip
```

PHP 程序

A、数据设备录入功能 : ①单个设备录入, ②批量设备录入。

B、数据设备配置批量备份。

数据设备录入功能 : 将数据设备录进数据库

单个设备录入功能

只需要填入 IP 地址, 选择设备型号即可, 添加设备时做以下几个操作。

1) 检查数据库中 IP 是否存在, 存在不添加, 不存在则添加进数据库。

2) 通过 SNMP 获取设备的主机名 (hostname)、主机描述 (description) 等信息。

3) 写进数据库的字段有 ip、hostname、description、version、device_type、model。

4) 部分 php 代码如下 :

```
$ip=$_POST['ip']; //ip 地址
$hostname=snmpget ($str, "popeye", "sysName.0");
```

// 获取设备 hostname

```
$description=snmpget ($str, "popeye", "sysDescr.0");
// 获取系统信息 description
```

// 向数据库添加一台新的设备

```
$sql = "INSERT INTO `device_table` (`ip`,
`hostname`, `description`, `version`, `device_type`,
`model`) VALUES ('$ip', '$hostname', '$description',
'','','$device_type', '$device_model')";
```

批量设备录入功能

批量录入有个注意点 : 上传文件里的 ip, 只能是同一型号的设备, 并且选择好设备型号。

批量添加的 PHP 代码

```
$file = fopen ($filename, "r"); // 打开上传文档
```

```
while ( !feof ( $file ) ) // 轮询文档
{
    $ip=fgets ( $file );
    $sql = "INSERT INTO `device_table` ( `ip`,
`hostname`, `description`, `version`, `device_type`,
`model` ) VALUES ( '$ip', '$hostname', '$description',
`\"`, '$device_type', '$device_model' ) ";
    $rs = mysql_query ( $sql, $link );
    if ( !$rs ) {echo $ip." 添加失败 ";}
    else
    {echo $ip." 添加成功 ".$hostname."<br>;"}
}
```

数据设备配置批量备份

```
$sql = "SELECT `ip`, `hostname`, `model` FROM
`device_table` WHERE 1";
```

/* 历遍数据库 device_table 表, 取出三个有用的字段 ip: 用于 telnet ; hostname : 配置文件名 ; modem : 选择 shell 脚本的变量。*/

```
$rs_sql = mysql_query ( $sql, $link );
while ( $row = mysql_fetch_row ( $rs_sql ) ) {
    $ip= $row[0];
    $hostname=$row[1];
    $model=$row[2];
    $str=exec ( "timeout 20 sh device_shell/$model.sh $ip
$hostname", $return_array, $return_status );
}
```

```
$str=exec ( "timeout 20 sh device_shell/$model.sh $ip
$hostname", $return_array, $return_status );
```

PHP 程序调用 linux shell 脚本, 并传二个变量, \$ip, \$hostname。

自动备份相关服务安装事项

TFTP 服务的配置

配置如下 : cat /etc/xinetd.d/tftp

```
service tftp
{
    disable = no
    // 开启 tftp 服务
    socket_type = dgram
    protocol = udp
    wait = yes
```

```
user = root
server = /usr/sbin/in.tftpd
server_args = -s /configuration -c -v // 指定配置存放文件夹
per_source = 11
cps = 100 2
}
samba 服务的配置
vim /etc/samba/smb.conf
[config_backup]
comment = Public Stuff
path = /configuration
browseable = yes
public = yes
writable = yes
printable = no
```

防火墙的配置

首先默认策略 :

```
iptables -P INPUT DROP
iptables -P FORWARD DROP
iptables -P OUTPUT DROP
```

然后添加允许的网段、端口。我的防火墙策略写得不是很细, 只是开放相关网段。

设备网段允许服务器主动请求出去, 不允许设备网段主动请求服务器。

```
iptables -A INPUT -s 192.168.10.0/19 -m state --state
NEW, ESTABLISHED -j ACCEPT
iptables -A OUTPUT -d 192.168.10.0/19 -m state --state
NEW, ESTABLISHED -j ACCEPT
办公网段全放开
iptables -A INPUT -s 192.168.20.0/24 -j ACCEPT
iptables -A OUTPUT -d 192.168.20.0/24 -j ACCEPT
```

应用实例

2016 年 2 月 1 日已经在现网中实际使用, 176 台数据设备, 配置在 20 分钟内全部保存完毕。

ShuoFang_S8600> 192.168.10.3ShuoFang_S8600 成功

192.168.10.4Shuo Fang_S8600_2 失败 124

HouZhai_S8600_1> 192.168.10.5HouZhai_S8600_1
成功

综述

由于开发了此自动备份程序，在很大程度上为网络

设备的稳定运行提供了强有力的保障。大大减少了网络中断时间以及网络故障的影响面，网络运营商的品牌形象得到了进一步的提高。

巧用 NQA 联动解决故障

北京 何涛 徐京渝

作者所在单位由于业务的需要，在两个不同的地点都部署了主备核心交换机，并且都下挂着较为重要的业务系统，两地间互访频繁。所使用的交换机都为华三公司的 S7502E 交换机，软件版本为 5.20。

如图 1 所示，笔者单位分别在 X 地点和 Y 地点各部署了两台核心交换机，同一地点的两台交换机通过 trunk 互连，通过传输与异地的核心交换机相连，形成口字型组网，互连 IP 地址如图 1 所标注。

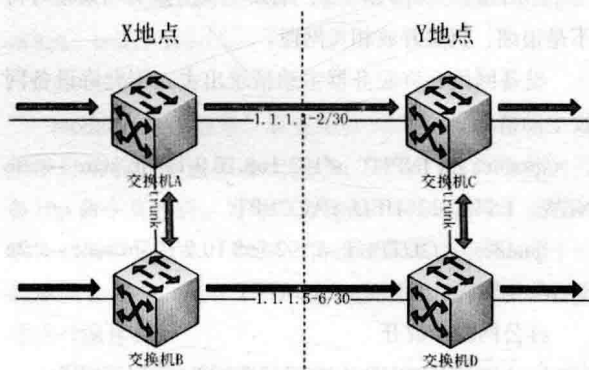


图 1 示意图

为了保证业务的可靠性，在正常情况下，数据从主路径通过，如图 1 中箭头所标注；当主路径出现故障时，数据从备路径通过，如图 1 中箭头所标注，或者先绕道核心交换机之间的心跳线，在从备路径通过，如图 1 中的双向箭头所标注。对于交换机 A 来说，当交换机 C 或者与交换机 C 之间的线路出现故障时，由于两地之间是通过传输相连，交换机 A 是无法感知到此故障的，此时如何保证数据自动切换到交换机 B 的备路径上来？

NQA (Network Quality Analyzer) 网络质量分析是一种实时的网络性能探测和统计技术，可以对响应时间、网络抖动、丢包率等网络信息进行统计，并将统计结果通知给其它模块，由其它模块来执行相关动作，从而实现联动。目前主流的交换机，包括华为、华三等国产设备都已经支持此项技术。在图 1 所示的场景中，我们可以通过在交换机 A 上部署静态路由与 NQA 的联动，来实现异地线路故障的自动路径切换。

正常情况下，交换机 A 通过下一跳 1.1.1.2 通往 Y 地点的网络，而将交换机 B 作为备份下一跳，表现在交换机配置上为：

```
ip route-static network mask 1.1.1.2
ip route-static net work mask 10.10.1.253 preference
70
```

静态路由配置命令的默认优先级为 60，将备份路由优先级配置为 70 的目的就是为了保证在缺省状态下不被激活，而当主路由失效时，备份路由会立即替代主路由而被激活。其中，10.10.1.253 是交换机 B 上一个 VLAN 的 IP 地址，对应在交换机 A 上的同网段 IP 地址为 10.1.1.252。

接下来，我们要做的就是通过配置将 NQA 与这条静态路由进行联动，首先我们得创建一个 NQA 探测组，并配置相应的参数，如下例所示：

```
nqa entry admin toSwitchC
//admin 是管理名，toSwitchC 是操作标签
type icmp-echo
```

```
// 探测类型, 这里即 ping 操作
destination ip 1.1.1.2
// 探测的目的 IP 地址
frequency 5000
// 探测频率为 5000ms
history-record enable
// 开启历史记录功能
history-record number 10
// 历史记录缓存为 10 条
probe count 10
// 每组探测次数
probe timeout 500
// 每次探测的超时时间
reaction 1 checked-element probe-fail thresh old-type
consecutive 3 action-type trigger-only
// 配置反应组 1, 探测失败 3 次则触发相应动作
在完成了 NQA 探测组的配置之后, 我们还需要配置跟踪组, 然后将跟踪组与对应的静态路由绑定, 这样才完成了联动功能的部署, 如下例所示:
```

```
track 1 nqa entry ad min toSwitchC reaction 1
// 将跟踪组与配置的 NQA 绑定
ip route-static net work mask 1.1.1.2 track 1
// 静态路由联动跟踪组
```

在完成了以上的配置后, NQA 与静态路由联动已经配置完成, 但还需要加上下面这条命令, 表示此探测组从现在开始生效, 并且持续有效:

```
nqa schedule admin toSwitchC start-time now lifetime
forever
```

工作流程

在设备运行过程中, 当交换机 A 与交换机 C 之间的传输链路出现故障, 导致数据无法传输, 此时交换机 A 无法 ping 通交换机 C 的 1.1.1.2 的接口 IP 地址, 在完成 3 次探测组的动作后, 如果发现还是无法到达 1.1.1.2, 则触发反应组 1 的动作, 下一跳为 1.1.1.2 的静态路由失效, 下一跳为 10.10.1.253 的静态路由生效, 数据通过备路径进行传输; 当交换机 A 与交换机 C 之间的链路恢复正常后, 交换机 A 可以 ping 通交换机 C 的 1.1.1.2 的接口 IP 地址, 则下一跳为 1.1.1.2 的静态路由恢复正常, 下一跳为 10.10.1.253 的静态路由相应失效。

按照同样的配置, 我们也可以对其它需要备份的链路进行保护, 从而实现故障期间的自动切换。

结语

综上所述, 我们可以利用 NQA 与静态路由的联动功能来完成对传输路径的保护, 但首先我们需要保证有一条备份路径供使用, 这样才能在主路径出现故障时, 利用此联动触发特性来自动失效主路由, 并切换到备路由上, 从而保证数据业务传输的正常进行。



系统网络端口安全防护

福建 荣世辉 李贵华 赖文鑫

常用端口及分类

电脑在因特网上相互通信需要使用 TCP/IP 协议, 而电脑总共有 65536 个端口, 这些端口分为 TCP 端口和 UDP 端口两种。按照端口号划分, 它们又可分为系统保留端口和动态端口两大类。其具体划分如下:

系统保留端口 (0-1023)。这些端口不允许用户私

自使用, 因为在系统层面上它们都有确切的定义, 一个或者多个端口号对应着因特网上常见的一些服务, 即每一个打开的端口都代表一个系统服务, 如 80 端口就代表 Web 服务, 21 对应 FTP, 25 对应 SMTP, 110 对应 POP3。

动态端口 (1024-65 53 5)。这些端口号是动态的, 当用户需要与别人通信时, Windows 系统会从 1024

起,在本机上分配一个动态端口,如果 1024 端口未关闭,再需要时就会分配 1025 端口供用户使用,依此类推。但有个别的系统服务会绑定在 1024-49151 的端口上,如 3389 端口为远程终端服务。从 49152-65535 端口,通常没有捆绑系统服务,允许 Windows 动态分配使用。

查看本机开放的端口

在默认状态下,Windows 系统会打开很多“服务端口”,如果用户想查看本机打开了哪些端口、有哪些电脑正在与本机连接,可以使用以下两种方法。

方法一:利用 Netstat 命令。Windows 系统提供了 Netstat 命令,能够显示当前的 TCP/IP 网络连接情况,前提条件是只有安装了 TCP/IP 协议才能使用 Netstat 命令。

操作方法:单击“开始→程序→附件→命令提示符”,进入 MS-DOS 窗口,输入命令 Netstat-na 回车,就会显示本机连接情况及打开的端口。其中 Local Address 代表本机 IP 地址和打开的端口号;Foreign Address 是远程计算机 IP 地址和端口号;State 表明当前 TCP 的连接状态;Listening 是监听状态,表明本机正在打开 135 端口监听,等待远程电脑的连接。如果在 DOS 窗口输入了 Netstat-na 命令,还将显示每个连接都是由哪些程序创建的。

如本机在 135 端口监听,就是由 Svchost.exe 程序创建的,该程序一共调用了 5 个组件(WS2.32.dll、RPCRT4.dll、rpcSS.dll、Svchost.exe、ADVAPI32.dll)来完成创建工作。如果发现本机打开了可疑的端口,就可以用该命令查看它调用了哪些软件,然后检查各组件的创建时间和修改时间,如果发现异常则电脑就可能被植入了木马病毒。

方法二:使用端口监视类软件。与 Netstat 命令类似,端口监视类软件也能查看本机打开了哪些端口,这类软件非常多,如 TcpvIEW、Port Reportre、绿鹰 PC 万能精灵、网络端口查看器等。密切监视本机端口连接情况,这样就能及时发现非法连接,及时采取有效措施。

关闭本机不用的端口

默认情况下 Windows 系统有很多端口是开放的,一旦上网,黑客可以通过这些端口连接上用户电脑,因此为了提高安全性可以关闭不用的端口。这些端口主要有 TCP139、445、593、1025 端口,UDP123、137、138、

445、1900 端口,流行病毒的后门端口 TCP2513、2745、3127、6129,以及远程服务访问端口 3389。关闭方法如下:

关闭 137、138、139、445 端口。它们都是为共享而开放的端口,所以用户要把这些端口全部关闭。单击“开始→控制面板→系统→硬件→设备管理器”→“查看”菜单→显示隐藏的设备→非即插即用驱动程序→NetBIOS over TCPIP→在属性窗口中选“常规”→不要使用这个设备(停用)→确定,重新启动机器。

关闭 UDP123 端口。单击“开始→设置→控制面板→管理工具→服务→停止 SSDP Discovery Service。关闭 UIP123 端口,可以防范某些蠕虫病毒。

关闭 UDP1900 端口。在控制面板中双击管理工具→服务→停止 SSDP Discovery Service 服务。关闭 UDP1900 端口,可以防范 DDos 攻击。

关闭其他端口。用户可以用网络防火墙来关闭,或者在控制面板中双击管理→本地安全策略→选中“IP 安全策略,在本地计算机”→创建 IP 安全策略→关闭。

重定向本机默认端口,保护系统安全

如果本机的默认端口不能关闭,建议使用端口“重定向”功能来提高系统的安全性,即把该端口重定向到另一个地址,这样可以隐藏公认的默认端口,降低系统受破坏的几率。例如,若用户电脑上开放了远程终端服务(Terminal Server)端口(默认是 3389),可以将它重定向到另一个端口(如 1234)。具体操作方法如下:

首先是在本机上(服务器端)修改。定位到下列两个注册表项,将其中的 Port Number 全部改成自定义的端口(如 1234)即可。

[HKEY_LOCAL_MACHINE\SYSTEM\CurrentControl Set\Control\Terminal Server \ Wds \ rdp wd \ Tds \ tcp]

[HKEY_LOCAL_MACHINE\SYSTEM\CurrentControl Set\Control\Terminal Server \ Win Stations \ RDP-Tcp]

而后在客户机上修改,将远程登录端口修改成 1234。方法如下:依次单击开始→程序→附件→通信→远程桌面连接→选项→扩展窗口→填写相关参数→常规→另存为,将该连接参数导出为 .rdp 文件。用记事本打开该文件,在文件最后添加一行:server port:i:1234(这里填写用户服务器自定义的端口)。以后直接双击这个 .rdp 文件,便可以连接到服务器的这个定义端口了。

思科交换机架构探讨

北京 何涛 徐京渝

Cisco 6500 系列交换机体系架构

Cisco Catalyst 6500 系列是 Cisco 重要的智能多层模块化交换机，一台 6500 系列交换机主要包括：机框（机箱）、电源（可有双电源）、引擎卡（可有双引擎）、板卡（线卡）、接口模块等。由于该系列交换机采用模块化配置，企业用户可根据实际业务需求灵活选择。

机箱

机箱是 Cisco Catalyst 6500 系列的基础，它是所有引擎、线卡、电源、风扇的容器。Cisco Catalyst 6500 系列交换机提供 3 插槽、4 插槽、6 插槽、9 插槽和 13 插槽这 5 种类型的机箱，如图 1 所示。所有机箱都支持冗余交换管理引擎和冗余电源。

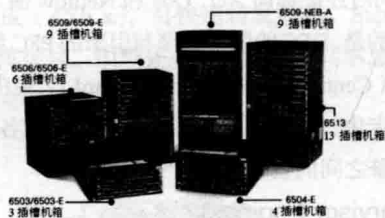


图 1 思科 6500 系列交换机机箱类型

Cisco Catalyst 6500 系列中的所有型号都使用了统一的模块和操作系统软件，形成了能够适应未来发展的体系结构，由于能提供操作一致性，因而能提高 IT 基础设施的利用率，并增加投资回报。其中，“E”系列支持更大的功率，可以带动更高的功率负载，支持更大的背板带宽，Cisco Catalyst 6500 的 E 系列包括 6503-E、6504-E、6506-E、6509-E、6513-E 这 5 种型号。如今，非“E”系列已经淡出了市场，下文主要针对“E”系列交换机进行阐述。

背板

如何使电源、引擎卡、线卡、接口模块这些模块相互连接起来呢？机箱的背板起到了至关重要的作用，可以把背板理解成各模块互联的通道。Cisco Catalyst 6500 系列有两种类型的背板，即 32 Gbps 的共享总线（Share

Bus）和交换矩阵（Switch Fabric）。

共享总线（Shared Bus）

Cisco Catalyst 6500 交换机的 32-Gbps 共享总线允许与之相连的所有端口发送和接收数据。共享总线实际上由三个独立的总线组成，即数据总线（DBus）、结果总线（RBUS）和控制总线（CBUS）。其中，DBus 是负责数据传输的主总线。在数据发送的过程中，所有已连接到背板的线卡都能捕获正被发送的数据，并且存储该数据包的副本。共享总线在数据交换的过程中，数据冲突不可避免，造成了数据交换的低效。RBUS 负责把引擎的操作结果转发给每个连接到背板上的线卡。CBUS 是控制总线，用于传输一些控制信息。

共享总线的背板连接器位于线卡的后端右侧。图 2 为两种线卡的共享总线背板连接器的位置示意图，左侧为 Cisco 的经典线卡，右侧为 CEF256 矩阵线卡（章节 2.4 中将详细介绍 Cisco Catalyst 6500 系列的常用线卡类型）。图中，框中标示出的为共享总线的背板连接器。

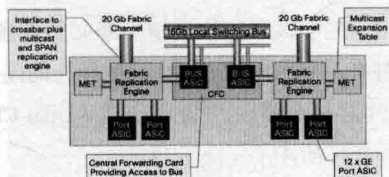


图 2 两种线卡的共享总线背板连接器的位置

交换矩阵（Switch Fabric）

交换矩阵与共享总线不同，共享总线为机箱标准的配置，而交换矩阵需要增加硬件的支持。随着技术的发展，交换矩阵经历了几次升级，第一代交换矩阵为独立的模块，交换矩阵模块（WS-C6500-SFM 和 WS-C6500-SFM2）提供 256 Gbps 的总交换容量。随着新的 Supervisor Engine 720 引擎的出现，交换矩阵模块已经融入了 Supervisor Engine720 引擎本身，省去了独立的交换矩阵模块。Supervisor Engine 720 引擎的集成交换矩阵模块的容量已从 256 Gbps 增加到 720 Gbps，而

2011 年发布的最新的 Supervisor Engine 2T 引擎的交换矩阵的容量增加至 2Tbps。

交换矩阵的背板连接器位于线卡的后端左侧，如图 3 所示。图中，框中标示出的为交换矩阵的背板连接器。

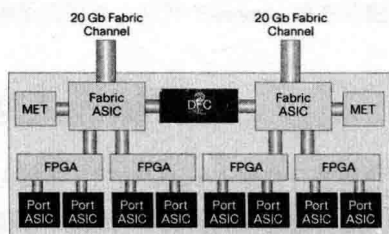


图 3 线卡的交换矩阵背板连接器的位置

背板与机箱槽位间的数据通路

Cisco 6509 为 Cisco Catalyst 6500 系列交换机中最常见的型号，图 4 为 Cisco 6509 这种 9 插槽的交换机的两种总线与机箱各个槽位的数据通路。

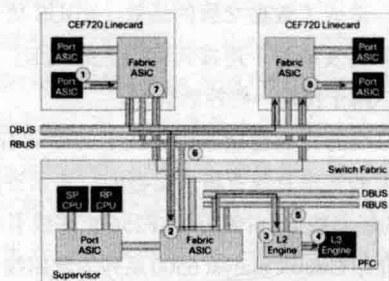


图 4 Cisco 6509 的共享总线、交换矩阵与各槽位间的数据通路

图 4 中，框中标示槽位表示引擎必须放置的位置，每个槽位都有与交换矩阵、共享总线相连的连接器，其中交换总线对每个槽位均为双通道（Dual Channels）。图 5 为交换矩阵的连接逻辑图。

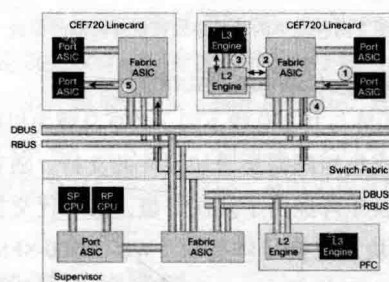


图 5 交换矩阵逻辑连接图

Supervisor Engine720 的每通道的交换能力为 20Gbps（单向），那么从图 5 可以推断出这个引擎的交换能力为： $20\text{Gbps} \times 2 \times 2 \times 9 = 720\text{Gbps}$ （双向、双通道、

9 个槽位）。

引擎（Supervisor）

Cisco Catalyst 6500 的引擎是负责软件加载、集中控制、数据处理的重要模块。交换能力的大小是判断引擎性能高低的主要指标，性能较高的引擎可以同时支持共享总线和交换矩阵这两种背板，性能较低的引擎只支持共享总线，这种引擎的交换能力最大为 32Gbps。下面详细介绍 3 种主流 6500 系列的引擎。为了更好的了解引擎的内部结构，先介绍以下几个概念：

控制面板（Control Plane）：引擎中的功能模块，负责控制数据的流向，生成路由表，一般由软件控制，操作软件在这里运行。MSFC（Multilayer Switch Feature Card/ 多层交换功能卡）就是控制面板。

数据面板（Data Plane）：引擎中的功能模块，根据控制面板给出的指令，完成数据转发、数据的质量管理、控制列表等。数据面板一般由硬件构成（ASICs），可以快速转发数据。PFC（Policy Feature Card/ 策略功能卡）就是一种数据面板，PFC 包括二层转发引擎、三层转发引擎。

DFC（Distributed Forwarding Card）：分布式转发卡，配置在线卡中，相当于本地转发引擎，可提高线卡的转发效率，同时还能提高 Acl、Qos 和 Netflow 的工作效率。值得注意的是，DFC 的版本必须与引擎的 PFC 版本一致。

CFC（Centralized Forwarding Card）：集中转发卡，配置在线卡中，配合引擎使用，提供线卡的各模块与共享总线引擎之间的数据通路。

Supervisor Engine 32

Supervisor Engine 32（下文简称 Sup 32）只支持 32 Gbps 的共享总线，提供 15Mpps 的转发速率。Sup 32 默认提供了一个集成的 PFC3B 数据面板和 MSFC2A 控制面板。图 6 为两种不同版本的 Sup 32 引擎，左侧的 WS-SUP32-GE-3B 配有 8 个千兆位以太网端口，右侧的 WS-SUP32-10GE-3B 配有 2 个 10Gb 以太网端口。



图 6 Sup 32 的两种版本

注意

PFC3B 中的 3B 为版本号, 每个版本有差别, 不同的引擎支持不同的版本, 具体详见思科官方网站。

Supervisor Engine 720

Supervisor Engine 720 (下文简称 Sup 720) 于 2003 年推出, 它把交换矩阵模块、PFC3、MSFC3 集成到一个模块中, 如图 7 所示。Sup 720 的交换矩阵容量为 720 Gbps, 可支持连接到不同类型的线卡, 如: 早期的线卡、每通道 8 Gbps 的线卡、每通道 20 Gbps 的线卡 (关于线卡的分类, 章节 2.4.1 中会详细描述)。Sup 720 引擎支持的集中式转发速率可达 30Mpps, 分布式转发速率高达 400Mpps, 分布式转发的速率需要与引擎版本相同的线卡的 DFC 配合。Sup 720 引擎是现阶段最常用的引擎, 图 7 为 Supervisor Engine 720 引擎。图中所示的 MSFC 负责控制数据的流向, 生成路由表, 操作软件在这里运行, 所有的操作都由 MSFC 的 CPU 调度。控制面板主要是软件控制, 需要大量计算工作。PFC 负责根据 MSFC 的计算结果进行数据转发, 以及数据的质量管理、控制列表等, PFC 就是引擎的数据面板, 数据面板由硬件构成 (ASICs), 可快速转发数据。Sup 720 集成了交换矩阵模块。引擎还有交换矩阵和共享总线的连接器, 图中未标出。

交换矩阵的背板连接器



矩阵线卡

图 7 Supervisor Engine 720

图 8 为 Sup 720 的内部体系, 该引擎的 MSFC 有两个 CPU, 一个为 RP, 一个为 SP, RP 用于三层数据交换, SP 用于二层数据交换, 思科的 iOS 就在 MSFC 中保存并运行, 在 iOS 中可以分别查看 RP 与 SP 的利用率。PFC 负责数据转发和控制, 包括了二层转发引擎和三层转发引擎。

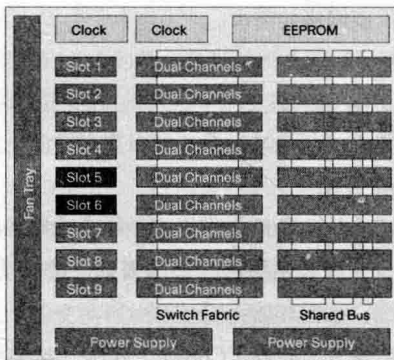


图 8 Supervisor Engine 720 内部体系

Sup 720 系列引擎中, 型号为 VS-SUP720-10G 的引擎支持思科虚拟交换系统 VSS1440。通过 VSS1440, 我们可以把硬件配置相同的两台 6500 系列交换机虚拟成一台交换机, VSS1440 系统能有效减少网络收敛时间、加快冗余切换速度等。

Supervisor Engine 2T

以 720 系列引擎和 6700 系列线卡为代表的上一代 Cisco Catalyst 6500 在应对日新月异的网络应用需求时, 逐渐显现出力不从心。为此, 思科于 2011 年 7 月发布了全新 Cisco Catalyst 6500 Supervisor Engine 2T (以下简称 Sup 2T) 管理引擎及配套的全新 6900 系列线卡, 在性能和功能上进行了大量的增强和创新, 图 9 为 Sup 2T 引擎示意图。

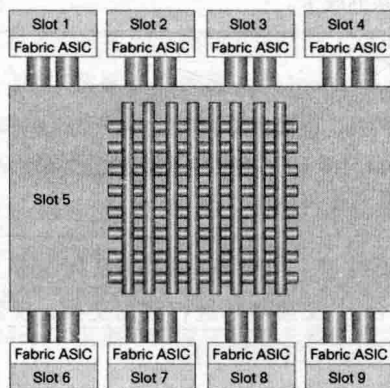


图 9 Supervisor Engine 2T 引擎

Sup 2T 集成了高性能交换矩阵, 全新 6900 系列线卡可在所有 6500 E 系列机箱内实现每个插槽 80 Gbps (双工 160Gbps) 的交换容量, 其转发引擎能够为 2 层和 3 层服务提供高性能转发。Sup 2T 在安全、服务质量 (QoS)、虚拟化和可管理性等方面提供了许多新的基于硬件的创新, 其丰富的功能集增强了传统 IP 转发、2 层和 3 层多协议标签交换 (MPLS) VPN、VPLS 等应用, 同时提供了可扩展的性能以满足无边界网络、数据中心

和服务提供商网络的需求。

Cisco 常用线卡

线卡的分类

Cisco Catalyst 6500 提供了多种线卡选择,以满足部署在接入、分配和网络核心层的需要。按照功能划分,思科 6500 系列线卡包括以下几类。

第一类线卡:经典(Classic)线卡,这类线卡只具有连接到 32Gbps 共享总线的连接器。无论机箱背板上有没有交换矩阵,这类线卡都不与交换矩阵有任何联系。经典线卡的代表有 WS-X61xx、WS-X63xx、WS-X64xx。

第二类线卡:这类线卡同时具有连接到 32 Gbps 共享总线和交换矩阵的连接器。若交换矩阵存在,这类线卡将使用交换矩阵进行数据交换;若不存在交换矩阵时,它会使用 32 Gbps 共享总线进行数据交换。第二类线卡的代表有 CEF256 系列线卡、CEF720 系列线卡。

第三类线卡:这些线卡不与共享总线连接,只能用交换矩阵完成数据交换,因此,使用这类线卡的交换机上必须有交换矩阵。这类线卡配置了本地交换引擎 DFC,本地交换的任务由 DFC 实现,大幅度提高了 pps(包转发率)。第三类线卡的代表有 dCEF256 系列线卡、dCEF720 系列线卡。

注意

CEF720、dCEF720 线卡连接到交换矩阵的通道是 20Gbps,而 CEF256、dCEF256 线卡连接到交换矩阵的通道是 8Gbps。

第四类线卡:主要为 dCEF2T 系列线卡。这类线卡只能配合 2T 交换矩阵进行数据交换,现阶段只有 Supervisor Engine 2T 引擎支持。

按照线卡的发展年代区分,第一代线卡为经典线卡,第二代线卡为交换矩阵通路为单路 8Gbps 的线卡,第三代线卡为交换矩阵通路为双通路 20Gbps 的线卡,第四代线卡为交换矩阵通路为双通路 40Gbps 的线卡。

线卡支持清单参考: http://www.cisco.com/c/en/us/td/docs/swit ches/lan/catalyst6500/hardware/Module_Installation/Mod_Install_Guide/6500-emig/02eth ern.html

常用线卡结构图

CEF720 线卡

图 10 所示的 CEF720 线卡是一个 48 口的千兆电口线卡,每 12 口一组芯片,每两组芯片使用一个复制引擎(Fabric Replication Engine),复制引擎跟交换矩阵相连,共享总线通过 CFC 卡与复制引擎相连。这类线卡没有数据面板,即没有数据转发引擎,所有的数据转发必须经过引擎的 PFC 模块进行转发。这类线卡的数据转发为集中转发方式,关于集中转发的详细描述可参加章节 3.1。



图 10 CEF720 线卡内部结构

dCEF720 线卡:

图 11 所示为 dCEF720 线卡,这类线卡没有与共享总线相连的端口,线卡内的复制引擎与 DFC 卡相连,DFC 必须与引擎中的 PFC 版本一致,DFC 通过交换矩阵与 PFC 数据同步,DFC 作为线卡的数据转发引擎对数据进行转发。这类线卡的数据转发为分布式转发方式,关于分布式转发的详细描述可参见章节 3.2。

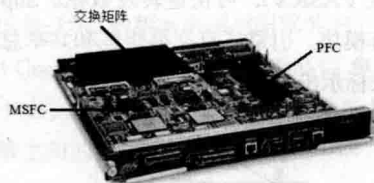


图 11 dCEF720 线卡内部结构

线卡架构混合使用

以最常见的 Sup 720 引擎为例,交换矩阵到每个通道的交换能力为 8 Gbps 或 20 Gbps,这由 Sup 720 时钟来控制,时钟速度是由线卡(CEF256 或 CEF720)来确定的。CEF256 和 dCEF256 线卡使 Sup 720 的交换矩阵时钟以 8 Gbps 工作,CEF720 和 dCEF720 线卡使 Sup 720 的交换矩阵时钟以 20 Gbps 工作。因此,Sup 720 交换矩阵可同时支持多个线卡在不同的插槽以不同的时钟速度运行,这意味着 Sup 720 可以支持单通道的 CEF256 线卡以 8 Gbps 工作以及双通道的 CEF720 线卡以 2×20 Gbps 工作,所有的 Sup 720 模块,最大提供 40 Gbps 的带宽给每个线卡插槽,为了向下兼容,Sup 720 引擎也支持经典线卡,这类线卡使用共享总线进行数据通信。

线卡间的数据包流向

为了更加深刻的理解线卡与引擎之间的关系，下面列举了两种常用的场景说明数据包的流向。

集中转发的数据流向

集中转发是使用引擎的 PFC 模块进行数据转发，每个线卡的转发流量都需要经过引擎的数据面板，如图 12 所示。这类线卡不包含 DFC 模块。

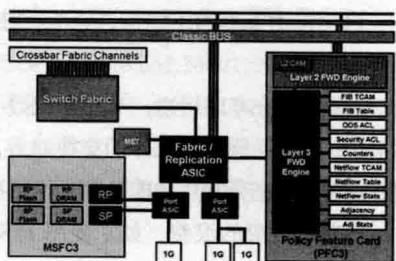


图 12 集中转发的数据流向图

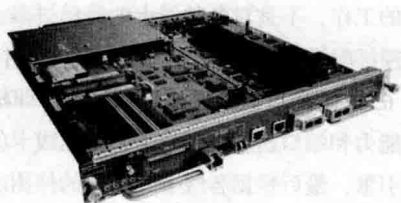


图 13 分布式转发的数据流向图

下面对图 12 中的每个数据转发步骤进行详细描述：

1. 数据到达端口进入线卡的交换模块。
2. 线卡的交换模块通过 DBus 总线传输数据的包头（不包括数据块），所有槽位的线卡都可以接受到这个包头信息。
3. 引擎接受到包头信息，将包头转发到 2 层交换引擎进行处理。
4. 2 层交换引擎转发包头信息到 3 层交换引擎，3 层交换引擎负责 Qos 控制，ACL 控制等等。
5. PFC 将处理结果通过 RBUS 返回引擎。
6. 引擎通过 RBUS 转发处理结果到所有的连接的线卡。
7. 当原数据线卡接受到处理结果，线卡将按照要求通过交换矩阵转发完整数据到目的线卡。
8. 目的线卡通过交换矩阵接受传输来的数据，并转发到对应的端口。

分布式转发的数据流向

分布式转发是使用线卡的 DFC 模块进行数据转发，数据转发不需要引擎的 PFC 参与，大大加快了数据交换

的效率。

下面对图 13 中的每个数据转发步骤进行详细描述：

1. 数据到达端口进入线卡的交换模块。
2. 线卡的交换模块转发数据包的包头给本地的 DFC 模块。
3. 本地 DFC 模块对数据的包头进行处理，包括路由、Qos、ACL 等等，将处理的结果返还到线卡的交换模块。
4. 线卡的交换模块通过交换矩阵发送完整的数据到目的线卡。
5. 目的线卡接受数据包并转发到对应的端口。

分布式转发不使用共享总线，数据流向简单快捷，减少了引擎的 PFC 卡的工作压力，大大提高了数据转发的效率。

Cisco Catalyst 6500 系列与其他系列的区别 思科 6500 与 4500 区别

思科 Cisco Catalyst 6500 交换机是针对大型企业核心网络 / 数据中心建设所需要的高端口密度、高转发性能、高级智能特性而开发的，其机箱、电源、内部交换架构均是依据大型企业核心网络和数据中心的应用特点而特别优化设计的。而思科 Catalyst 4500 系列产品则不同，它通常用作中小型企业核心设备或大型网络的汇聚层设备。6500 与 4500 的具体区别主要体现在如下几个方面。

性能

6500 系列交换机的交换能力可达到 720Gbps（每槽位 40G），IPV4 数据包吞吐量 450Mpps（基于硬件）；而且 MAC 地址表的容量能够达到 64K，IPV4 路由表最大达到 1M（仅仅基于 720 引擎）。

4500 系列交换机即使采用思科最新推出的 Supervisor Engine 6-E 引擎，其交换能力最大也只能达到 320Gbps（每槽位最大 24G），IPV4 包转发率也只能达到 250Mpps，其整体性能与 6500 E 相比相差甚远。

硬件架构

6500 E 的交换架构为无阻塞的交换矩阵架构（Switch Fabric），通过交换矩阵架构，交换机各插槽的线卡能够实现点到点的分布式转发，数据交换效率大大提高。

4500E 采用的仍然是传统的总线架构（Classic BUS），交换机各插槽线卡间的通信需要经过一条共享带宽的总线，由交换机控制引擎进行统一调度，它的缺点在于整个交换机的路由性能受限于总线带宽和控制引擎，数据交换能力低下，而且加重了交换机控制引擎的负担。这种传统的总线架构正逐步被先进的交换矩阵架

构所取代。

此外, 4500E 系列交换机中仅有 4507R-E 和 4510R-E 支持双引擎, 而 6500E 系列交换机中的所有型号均支持冗余的双引擎。

数据中心应用关键特性

为了强化交换网络中的核心层设备, Cisco 推出了 VSS 技术(虚拟交换技术), VSS 的功能是将多台交换机虚拟成单台交换机, 在配置 VSS 之后, 不仅可以提高核心交换机的易操作性, 同时还能实现核心层的故障恢复率, 从而提供不间断通信能力。在配置 VSS 之后的多台交换机之间不再有冗余设备, 而是所有交换机都同时工作, 最终扩展整体核心交换能力。

这种功能特性在企业数据中心的应用中相当先进和实用, 目前仅有 6500 系列交换机支持这种特性(只有配备了 VS-SUP720-10G 或 Supervisor Engine 2T 引擎, 才支持 VSS), 2 台配备了 VS-SUP720-10G 引擎的 6500 交换机配置 VSS 之后的核心交换能力可以达到 1440Gbps, 是原来单台设备的 2 倍。4500 系列交换机尚不能支持 VSS 特性。

服务模块

作为企业网络中的核心设备, 为了安全和管理方便, 经常需要在交换机上部署相应的功能模块, 如防火墙模块、入侵检测模块、流量分析模块、无线控制器模块等, 目前只有 6500 系列交换机支持这些服务模块, 以上服务模块 4500 交换机均不能支持。

思科 6500 与 7600 区别

7600 系列交换机侧重于路由功能, 对数据包的快

速转发进行了优化, 在 ACL、Qos 等控制方面功能强大。6500 主要侧重交换功能, 对数据的二层交换能力强, 6500 使用在企业网核心交换, 负责大量数据的快速交换, 而 7600 更对应用在边界, 支持更多的广域网接口, 更高效的数据控制。7600 系列路由器支持更多的广域网接口, 7600 系列是在 6500 系列的基础上开发出来的, 因此大部分的线卡可以互用。

结语

设备选型应该充分考虑用途, 对交换能力有清晰的认识, 交换引擎的交换能力是总体的交换能力, 只有在合理的搭配情况下, 充分利用才能达到交换的峰值, 若使用不当, 会带来资源的浪费, 如: 使用了 Supervisor Engine720 引擎, 但是配了一个或多个经典线卡, 这样会大大的拖累整个系统的交换能力。因此, 设备选型是一个细致的工作, 不是对各种线卡的简单拼凑, 需要根据需求合理搭配线卡、引擎、电源功率。本文作者认为, 选择思科 6500 系列应该遵循这样的流程, 即根据需求确认交换能力和端口密度选择线卡, 根据线卡的总交换能力选择引擎, 最后根据各线卡和引擎的使用功率来选择机箱和电源。总之, Cisco Catalyst 6500 系列的选型是一个细致而专业的过程, 需要对体系有较深的了解, 希望此文可以对大家选型 Cisco Catalyst 6500 系列交换机有所帮助。

链路聚合扩带宽

山东 何钰 李绪军

近日经过网管平台对 BRAS 设备端口流量的记录, 我们分析得知 BRAS 连接以太网传输设备的端口带宽利用率已经达到 80% 以上, 这就急需我们扩大该链路带宽。增加链路带宽的方法其一就是更换物理端口, 例如原来使用的是千兆端口, 更换成万兆端口; 第二个办法

就是使用链路聚合的办法解决, 经过比较, 更换物理端口除了价格高昂外, 传输设备上并没有万兆端口, 这样的话我们就使用链路聚合来解决这一问题。首先我们配置 BRAS 设备, 需要在 BRAS 上的操作主要分为链路聚合子接口的创建、子接口 VCC 配置以及子接口 VLAN

的封装,最后再将两个物理端口加入到我们定义的链路聚合组即可。按照这一思路我们首先创建子接口具体配置即:

```
interface smartgro up2.78
// 创建链路聚合组的子接口 2.78
interface smartgro up2.79
// 创建链路聚合组的子接口 2.79
interface smartgro up2.10001999
// 创建链路聚合组的子接口 2.10001999
interface smartgro up2.20002999
// 创建链路聚合组的子接口 2.20002999
```

上面我们完成了 smartgroup 组子接口的创建,接下来我们再配置子接口的 VCC 即用户侧电路,具体配置即:

```
vcc-configuration
// 进入 VCC 配置模式
interface smartgro up2.78
// 进入 VCC 接口业务配置模式
Interface smartgroup 2.79
// 进入 VCC 接口业务配置模式
interface smartgro up2.10001999
// 进入 VCC 接口业务配置模式
pre-domain dhcp
// 配置认证前默认域为 DHCP
encapsulation ip-over-ethernet
// 接入封装类型为 IPoE, 只允许 DHCP 用户接入
interface smartgro up2.20002999
// 进入 VCC 接口业务配置模式
encapsulation ppp-over-ethernet
// 接入封装类型为 PPPoE, 只允许 PPPoE 用户接入
pppox template 1
// 绑定模板
```

刚才我们完成了子接口 VCC 的配置,最后我们将封装该子接口的 VLAN 信息具体配置即:

```
vlan-configuration
// 进入 vlan 配置模式
interface smartgro up2.78
// 进入 VLAN 子接口业务配置模式
encapsulation-dot1q 78
// 封装端口 vlan
interface smartgro up2.79
// 进入 VLAN 子接口业务配置模式
```

```
encapsulation-dot1q 79
// 封装端口 vlan
interface smartgro up2.10001999
// 进入 VLAN 子接口业务配置模式
user-dynamic-vlan any-other-qinq
// 为新创建的 VCC 子接口配置动态 VLAN 标记,
支持双层的动态 VLAN 功能
qinq range internal-vlan-range 1000-1999 external-
vlan-range 1000-1999
// 配置多段内外层 VLAN 标签
interface smartgro up2.20002999
// 进入 VLAN 子接口业务配置模式
user-dynamic-vlan any-other-qinq
// 为新创建的 VCC 子接口配置动态 VLAN 标记,
支持双层的动态 VLAN 功能
qinq range internal-vlan-range 2000-2999 external-
vlan-range 2000-2999
```

// 配置多段内外层 VLAN 标签

这样我们就完成了子接口的创建、端口 VCC 的配置以及子接口 VLAN 的封装,最后我们在将两个物理端口加入到 smartgroup2 中。具体配置即:

```
Lacp
// 进入 LACP 配置模式
interface gei-0/0/1/6
// 进入端口
smartgroup 2 mode on
// 将端口加入链路聚合组 2, 模式为 on 即手动聚合
interface gei-0/0/1/7
// 进入端口
smartgroup 2 mode on
// 将端口加入链路聚合组 2, 模式为 on 即手动聚合
```

这里值得注意的是我们这里采用的是手动聚合方式,为什么要使用手动聚合模式呢?这是因为 BRAS 和传输设备是两个不同厂家的设备,为了保证设备间数据传输的稳定性,避免设备间不兼容性,通常不同厂家设备使用链路聚合时我们采用手动聚合的模式。

上面我们完成了 BRAS 设备链路聚合的配置,接下来我们将配置传输设备 CESP,这里我们需要先创建一个 TRUNK 组,然后在 TRUNK 组中加入相应的 VLAN 信息,最后将物理端口加入到 TRUNK 组中即可,接下来我们开始配置:


```

Config
// 进入配置模式
Interface trunk 1/1
// 创建 TRUNK 组
Join vlan    78, 79, 1000-1050, 2000-2050
tagged
// 在 TRUNK 组中加入相应的 VLAN
Interfacer gig1/17
// 进入端口 1/17
Join trunk1/1
// 将端口 1/17 加入到 TRUNK 组中
Interface gig1/18
// 进入端口 1/18
Join trunk1/1
// 将端口 1/18 加入到 TRUNK 组中
    
```

上面我们先后创建了 TRUNK 组、在 TRUNK 组中加入 VLAN 以及将端口加入到 TRUNK 组中，经过这些操作我们再将两侧的 4 个端口进行了速度和双工模式的强制后，端口和链路聚合组都已经 UP，我们在 BRAS

设备上使用命令，可以看到互联 CESP 的端口用户数量不断增加，这就说明互联网用户已经通过我们配置的链路聚合组端口交换数据了，同样我们在两侧设备上我们查看到流量已经在两个端口上进行了分流，这样就实现了我们增加链路带宽的目的。

刚才我们通过配置 BRAS 和 CESP 关于链路聚合的数据，达到了增加链路带宽的目的，同时也起到了流量的负载分担和链路保护的作用，起到了两全其美的效果。其实作为网络运维人员在网络部署的前期眼光要放长远些，后期为了避免因为带宽不足而增加端口的问题，我们在开通新的网络设备时，将根据实际情况直接采用链路聚合方式进行上联 BRAS，这样做的好处是在链路带宽拥塞的时候，我们只需要额外的增加一个物理端口到链路聚合组即可，这样既不会中断业务，操作起来也显得方便了许多。其实作为一个网络运维人员，有时候我们多考虑一点，把事情考虑的全面些，就会避免许多网络麻烦的发生，从而提高网络的可靠性打下良好的基础。

巧用批处理查找端口

广州 淡武强

作者所在单位要部署一套温湿度监控系统。该系统由华图 S400W 无线温湿度记录仪、HE2400 无线基站和监控软件组成。一个或多个无线温湿度记录仪探测环境温湿度，通过 RF 射频传送给该环境中的无线基站，无线基站经有线或无线局域网将监测数据通过 UDP 协议传送至监控服务器。客户端通过 B/S 结构可查看温湿度记录，接收报警。

该系统有 40 多个无线基站接入到二层交换机，局域网为核心、接入两层结构，接入层交换机有 30 多台，按部门划分了 30 多个 VLAN，为管理方便，部署中需将所有的无线基站划归同一 VLAN。如果手工为所有无线基站调整 VLAN、分配固定 IP，工作量庞大，因此想用批处理来实现。

实现思路

首先，每个无线基站均有 MAC 地址，先统一把所有无线基站逐一连接笔记本电脑，预先设置好固定 IP，192.168.31.0/24 网段，并记录下其 MAC 地址；

然后，将所有无线基站部署到各监测点，开机；

最后，在局域网中一台电脑上运行批处理程序，输入 MAC 地址，即可找到该基站所连接的交换机端口，将端口划至 VLAN 31。

批处理中需先 Telnet 至核心交换机，查找指定 MAC 所直连的二层交换机，再 Telnet 至二层交换机，找到该 MAC 所连接的端口，并修改端口的 VLAN 号。然而批处理在使用 Telnet 时无法自动输入 Telnet 登录密码，而 VBscript 脚本使用 SendKeys 命令能做到，因此

若把二者结合使用,就能达到想要的效果。网络拓扑如图1所示。

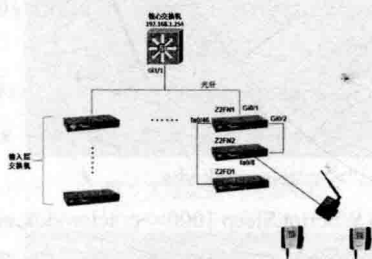


图1 网络拓扑图

FindMac.bat 批处理内容如下。

@rem 第一步:输入 MAC 地址, Telnet 核心交换机查找该 MAC 所连接的核心交换机端口

```
@set /p mymac= 请输入要查找的 MAC:
@del c:\telcore.vbs
@echo on error resum e next >>c:\telcore.vbs
@echo dim WshShell>>c:\telcore.vbs
@echo Set WshShell = WScript.CreateObject ("WScript.Shell") >>c:\telcore.vbs
@echo WshShell.run "cmd">>c:\telcore.vbs
@echo WshShell.App Activate "c:\windows\system32\cmd.exe">>c:\telcore.vbs
@echo WScript.Sleep 200>>c:\telcore.vbs
@echo WshShell.SendKeys "telnet 192.168.1.254{ENTER}">>c:\telcore.vbs
@echo WScript.Sleep 100>>c:\telcore.vbs
@echo WshShell.AppActivate "telnet.exe ">>c:\telcore.vbs
@echo WScript.Sleep 2000>>c:\telcore.vbs
@echo WshShell.SendKeys "jikon {ENTER}">>c:\telcore.vbs
@echo WScript.Sleep 2000>>c:\telcore.vbs
@echo WshShell.SendKeys "sh mac add add %mymac%{ENTER}">>c:\telcore.vbs
@echo WScript.Sleep 1000>>c:\telcore.vbs
@echo WshShell.SendKeys "sh cdp nei {ENTER}">>c:\telcore.vbs
@echo WScript.Sleep 1000>>c:\telcore.vbs
@call c:\telcore.vbs
@rem 第二步:输入二层交换机的管理 IP, 查找该 MAC 所连接的二层交换机端口
@cls
```

@set /p sw= 请输入该 MAC 所连接的二层交换机 IP :

```
@del c:\telsw.vbs
@echo on error resum e next >>c:\telsw.vbs
@echo dim WshShell>>c:\telsw.vbs
@echo Set WshShell = WScript.CreateObject ("WScript.Shell") >>c:\telsw.vbs
@echo WshShell.run "cmd">>c:\telsw.vbs
@echo WshShell.App Activate "c:\windows\system32\cmd.exe">>c:\telsw.vbs
@echo WScript.Sleep 200>>c:\telsw.vbs
@echo WshShell.SendKeys "telnet %sw%{ENTER}">>c:\telsw.vbs
@echo WScript.Sleep 100>>c:\telsw.vbs
@echo WshShell.App Activate "telnet.exe ">>c:\telsw.vbs
@echo WScript.Sleep 2000>>c:\telsw.vbs
@echo WshShell.SendKeys "jikong {ENTER}">>c:\telsw.vbs
@echo WScript.Sleep 2000>>c:\telsw.vbs
@echo WshShell.SendKeys "sh mac add add %mymac%{ENTER}">>c:\telsw.vbs
@echo WScript.Sleep 1000>>c:\telsw.vbs
@echo WshShell.SendKeys "sh cdp nei {ENTER}">>c:\telsw.vbs
@echo WScript.Sleep 1000>>c:\telsw.vbs
@call c:\telsw.vbs
@rem 第三步:输入二层交换机的管理 IP, 查找该 MAC 直连的二层交换机端口
@cls
@set /p swzl= 请输入该 MAC 所直连的二层交换机 IP :
@del c:\telswzl.vbs
@echo on error resume next >>c:\telswzl.vbs
@echo dim WshShell>>c:\telswzl.vbs
@echo Set WshShell = WScript.CreateObject ("WScript.Shell") >>c:\telswzl.vbs
@echo WshShell.run "cmd">>c:\telswzl.vbs
@echo WshShell.App Activate "c:\windows\system32\cmd.exe">>c:\telswzl.vbs
@echo WScript.Sleep 200>>c:\telswzl.vbs
@echo WshShell.SendKeys "telnet %swz
```

```

I%{ENTER}">>c:\telswzl.vbs
    @echo WScript.Sleep 100>>c:\telswzl.vbs
    @echo WshShell.AppActivate"telnet.exe">>c:\telswzl.vbs
vbs
    @echo WScript.Sleep 2000>>c:\telswzl.vbs
    @echo WshShell.SendKeys"jikong{ENTER}">>c:\telswzl.vbs
    @echo WScript.Sleep 2000>>c:\telswzl.vbs
    @echo WshShell.SendKeys"sh mac add add %mymac%{ENTER}">>c:\telswzl.vbs
    @echo WScript.Sleep 1000>>c:\telswzl.vbs
    @call c:\telswzl.vbs
    @rem 第四步：输入二层交换机端口号，修改 VLAN
    @cls
    @set /p swzldk= 请输入该 MAC 所直连的二层交换机端口号：
    @del c:\telswzldk.vbs
    @echo on error resume next>>c:\telswzldk.vbs
    @echo dim WshShell>>c:\telswzldk.vbs
    @echo Set WshShell =WScript.CreateObject("WScript.Shell")>>c:\telswzldk.vbs
    @echo WshShell.run "cmd">>c:\telswzldk.vbs
    @echo WshShell.AppActivate"c:\windows\system32\cmd.exe">>c:\telswzldk.vbs
    @echo WScript.Sleep 200>>c:\telswzldk.vbs
    @echo WshShell.SendKeys"telnet %swzl%{ENTER}">>c:\telswzldk.vbs
    @echo WScript.Sleep 100>>c:\telswzldk.vbs
    @echo WshShell.AppActivate"telnet.exe">>c:\telswzldk.vbs
    @echo WScript.Sleep 2000>>c:\telswzldk.vbs
    @echo WshShell.SendKeys"jikong{ENTER}">>c:\telswzldk.vbs
    @echo WScript.Sleep 2000>>c:\telswzldk.vbs
    @echo WshShell.SendKeys"en{ENTER}">>c:\telswzldk.vbs
    @echo WScript.Sleep 1000>>c:\telswzldk.vbs
    @echo WshShell.SendKeys"jikong{ENTER}">>c:\telswzldk.vbs
    @echo WScript.Sleep 2000>>c:\telswzldk.vbs
    @echo WshShell.SendKeys"conf t{ENTER}">>c:\telswzldk.vbs

```

```

telswzldk.vbs
    @echo WScript.Sleep 1000>>c:\telswzldk.vbs
    @echo WshShell.SendKeys"int f0/%swzldk%{ENTER}">>c:\telswzldk.vbs
    @echo WScript.Sleep 1000>>c:\telswzldk.vbs
    @echo WshShell.SendKeys"switaccevlan31{ENTER}">>c:\telswzldk.vbs
    @echo WScript.Sleep 1000>>c:\telswzldk.vbs
    @echo WshShell.SendKeys"no shut{ENTER}">>c:\telswzldk.vbs
    @echo WScript.Sleep 1000>>c:\telswzldk.vbs
    @echo WshShell.SendKeys"end{ENTER}">>c:\telswzldk.vbs
    @echo WScript.Sleep 1000>>c:\telswzldk.vbs
    @echo WshShell.SendKeys"wr{ENTER}">>c:\telswzldk.vbs
    @echo WScript.Sleep 1000>>c:\telswzldk.vbs
    @call c:\telswzldk.vbs
    @rem 清除所定义的变量
    @set mymac=
    @set sw=
    @set swzl=
    @set swzldk=

```

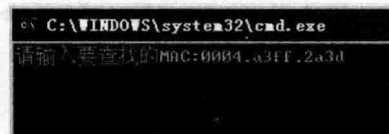


图2 输入 MAC 地址

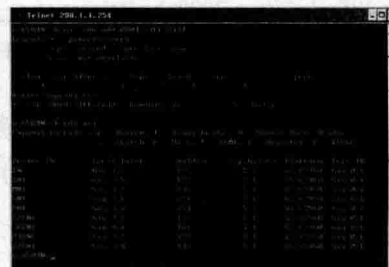


图3 核心交换机连接拓扑

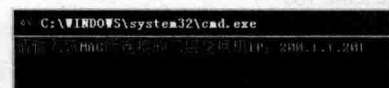


图4 输入二层交换机 IP 地址



图 5 二层交换机连接拓扑

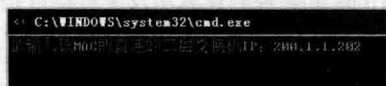


图 6 输入直连的二层交换机 IP 地址

批处理运行过程的解释：

第一步：定义变量 mymac，让用户从键盘输入无线基站的 MAC 地址，将第一段代码追加到 telcore.vbs 文件并调用，即 Telnet 核心交换机 192.168.1.254，查找该 MAC 所连接的核心交换机端口。

拓扑中显示核心交换机通过光纤连接了 9 台二层交换机，该 MAC 地址连接在 Gi3/1 端口所连接的二层交换机上，该二层交换机名称是 Z2FN1，对 telswzl.vbs 的调用完成。用户查找交换机 hostname 命名表，找到 Z2FN1 的 IP 是 192.168.1.201。

第二步：定义变量 sw，让用户从键盘输入二层交换机 Z2FN1 的管理 IP 地址 192.168.1.201，将第二段代码追加到 telsw.vbs 文件并调用，即 Telnet 二层交换机 192.168.1.201，查找该 MAC 所连接的二层交换机端口。

拓扑中显示二层交换机 Z2FN1 共连接了 3 台交换机，即 Gi0/1 口通过光纤连接核心交换机、Gi0/2 千兆电口连接二层交换机 Z2FN2、百兆电口 Fa0/46 连接二层交换机 Z2FD1。该 MAC 地址连接在 Gi0/2 端口所连接的二层交换机上，该二层交换机名称是 Z2FN2，对 telsw.vbs 的调用完成。用户查找交换机 hostname 命名表，

找到 Z2FN2 的 IP 是 192.168.1.202。

第三步：定义变量 swzl，让用户从键盘输入二层交换机 Z2FN2 的管理 IP 地址 192.168.1.202，将第三段代码追加到 telswzl.vbs 文件并调用，即 Telnet 二层交换机 192.168.1.202，查找该 MAC 直连的二层交换机端口。

显示该无线基站连接在 192.168.1.202 这台二层交换机的 Fa0/8 百兆电口上，对 telswzl.vbs 的调用完成。

第四步：定义变量 swzldk，让用户从键盘输入端口号 8，将第四段代码追加到 telswzldk.vbs 文件并调用，将端口加入 VLAN 31，启用端口并保存。

最后，删除所定义的 4 个变量。至此批处理结束。

如果网络拓扑为核心层、汇聚层、接入层的三层结构，此过程还要增加一个步骤。显然，该批处理还不够智能化，最理想的结果是用户只需输入 MAC 地址，所有的工作自动完成，因此尚需进一步优化，而其复杂度和代码量将大大增加。



图 7 找到端口号



图 8 输入端口号



图 9 将端口加入 VLAN31

❖ 链路聚合在局域网的应用

安徽 刘勇

某校园网核心层使用两台核心交换机，互为备，

汇聚层交换机按不同区域分别连接在这两台交换机上。

两台核心交换机之间通过链路互联实现数据传输，通过一段时间的观察，发现在网络使用高峰期时，两台交换机之间的链路上的流量达到 90% 以上，甚至引起拥塞，所以对这两台交换机之间的链路进行扩容刻不容缓。使用链路聚合技术可以有效增加带宽，提高冗余能力，有效达到缓解拥塞状态的目的。笔者浅述下链路聚合技术在局域网中的应用，希望对大家有所帮助。

我们以华为 S 系列交换机为例。链路聚合称之为 Eth-Trunk，是将一组相同类型的物理以太网接口捆绑打包在一起的逻辑接口，有两种类型的 Eth-Trunk 模式，一种为手工负载分担模式，一种为静态 LACP 模式，这两种模式的最主要区别为手工负载分担模式所有成员链路都处于转发状态，而静态 LACP 模式有非活动的备份链路。本文以手工负载分担模式为例。

物理层连接

任意选择交换机的空闲端口，例如选择 A 交换机的 GE0/0/1、GE0/0/2 两个物理端口，B 交换机的 GE0/0/1、GE0/0/2，通过尾纤进行一一连接，通过的 VLAN 为 100、200。

数据配置

步骤 1 创建 Eth-Trunk

创建 Eth-Trunk 1。

```
<SwitchA> system-view
```

```
[SwitchA] interface eth-trunk 1
```

```
[SwitchA-Eth-Trunk1] quit
```

步骤 2 向 Eth-Trunk 中加入成员接口

将 GE0/0/1 加入 Eth-Trunk 1。

```
[SwitchA] interface gigabitethernet 0/0/1
```

```
[SwitchA-GigabitEthernet0/0/1] eth-trunk 1
```

```
[SwitchA-GigabitEthernet0/0/1] quit
```

将 GE0/0/2 加入 Eth-Trunk 1。

```
[SwitchA] interface gigabitethernet 0/0/2
```

```
[SwitchA-GigabitEthernet0/0/2] eth-trunk 1
```

```
[SwitchA-GigabitEthernet0/0/2] quit
```

步骤 3 配置 Eth-Trunk 1

配置 Eth-Trunk 1 允许 VLAN 100 和 VLAN 200 的报文通过。

```
[SwitchA] interface eth-trunk 1
```

```
[SwitchA-Eth-Trunk1] port link-type trunk
```

```
[SwitchA-Eth-Trunk1] port trunk allow-pass vlan 100 200
```

```
[SwitchA-Eth-Trunk1] quit
```

重复同样的步骤配置 SwitchB。

步骤 4 验证配置结果

在任意视图下执行 display trunkmembership 命令，检查 Eth-Trunk 1 是否创建成功及成员接口是否正确加入。

```
[SwitchA] display trunkmembership eth-trunk 1
```

```
Trunk ID: 1
```

```
used status: VALID
```

```
TYPE: ethernet
```

```
Working Mode : Normal
```

```
Number Of Ports in Trunk = 2
```

```
Number Of UP Ports in Trunk = 2
```

```
operate status: up
```

```
Interface GigabitEthernet0/0/1, valid, operate up, weight=1,
```

```
Interface GigabitEthernet0/0/2, valid, operate up, weight=1,
```

显示 Eth-Trunk 1 的配置信息。

```
[SwitchA] display eth-trunk 1
```

```
Eth-Trunk1's state information is:
```

```
WorkingMode: NORMAL Hash arithmetic: According to SA-XOR-DA
```

```
Least Active-linknumber: 1 Max Bandwidth-affected-linknumber: 8
```

```
Operate status: Up Number Of Up Port In Trunk: 2
```

从以上信息看出 Eth-Trunk 1 中包含 2 个成员接口 GE0/0/1 和 GE0/0/2。成员接口的状态都为 Up，表明配置是成功的。

验证效果

经过网络高峰期的流量观测，Eth-Trunk 中的两条链路起到了理想的平均负载分担的作用，每条链路的拥塞率不超过 50%。

注意事项

要注意的是 Eth-Trunk 中的成员接口属性保持为默认属性；成员接口保持同一类型，或同为千兆，或同为

百兆；Eth-Trunk 链路两端必须都要配置；Eth-Trunk 中最多支持 8 条链路。



简化版的网络防火墙

宁波 姚明友

单位某部门采购了一台大型设备，此套设备有许多仪器组建成一个内部局域网，其中一台服务器是双网卡，一块用于它们系统的内部局域网交互，一块用于跟单位内部系统数据交互，这意味着这台服务器会跟单位内网物理连通，存在一定的安全隐患，笔者对外联设备要求比较严格，故让软件服务商敲定最终方案后，提供笔者外联服务器跟单位内部服务器交互的具体地址以及端口号，再通过 ACL 访问控制列表做安全实施。思虑之后想到两种方法可以满足需求。

在核心上对指定 VLAN 做 ACL 控制

笔者通过 Cisco Packet Tracer 软件模拟了一个类似的实验环境。

实验目的：让“中间服务器”只允许访问“内部服务器 1”的 WWW 服务。

为了便于描述，将“中间服务器”比为“A”，“内部服务器 1”比为“B”，“内部服务器 2”比为“C”

在未设置 ACL 时，A 能 Ping 通 B 跟 C。

当设置好 ACL 后，A 不能 Ping 通 B 跟 C，但能访问 B 的 www 服务。

三层交换机的 ACL 配置如下。

首先如图 1 所示创建 ACL 规则，再在 VLAN 端口上应用所创建的 ACL 规则，如图 2 所示。

```
ip access-list extended vlan33
permit tcp host 192.168.33.250 host 192.168.100.100 eq www
deny ip host 192.168.33.250 any
permit ip any any
```

图 1 创建 ACL 规则

```
interface Vlan33
ip address 192.168.33.254 255.255.255.0
ip access-group vlan33 in
```

图 2 应用 ACL 规则

其中 ACL 规则里的命令“Permit ip any any”是为了实验环境模拟方便，实际环境具体更改。

```
ip access-list extended vlan33
permit tcp host 192.168.33.250 host 192.168.100.100 eq www
```

图 3 创建 ACL 规则

```
interface GigabitEthernet1/0/19
switchport access vlan 33
switchport mode access
ip access-group vlan33 in
```

图 4 应用 ACL 规则

在接入层交换机上做 ACL 控制

由于模拟器无法在端口上应用 ACL，故在思科交换机模拟。

创建 ACL 的规则跟上面一样，区别是此 ACL 规则需应用在端口上，配置如下。首先如图 3 所示创建 ACL 规则，再在交换机端口上应用所创建的 ACL 规则如图 4 所示。

以上两种方法都可以满足需求，根据实际情况最终笔者选择了第二种方法，对单台设备控制更加准确、方便。第一种方法更适合对批量设备的控制。

❖ 用命令配置两张网卡

湖南 曹彩武

Route 命令是在本地 IP 路由表中显示和修改条目网络命令。看到这里，你肯定明白了吧，就是一台电脑，两张网卡，让这台电脑同时可以访问内、外网。访问完毕后，将内网网线拔下即可。

复习下 Route 命令：

语法：route [-f] [-p] [Command [Destination] [mask Netmask] [Gateway] [metric Metric]] [if Interface]

举例几条比较常用的：

route print

// 显示 IP 路由表的完整内容。

route add 0.0.0.0 mask 0.0.0.0 192.168.12.1

// 添加默认网关地址为 192.168.12.1 的默认路由；

route delete 10.41.0.0 mask 255.255.0.0

// 删除目标为 10.41.0.0，子网掩码为 255.255.0.0 的路由；

其次，说说我院的网络情况。

医保网网段：192.168.10.X 网关：192.168.10.1 子网掩码：255.255.255.0

互联网网段：192.168.60.X 网关：192.168.60.1 子网掩码：255.255.255.0

两个网段属于独立局域网。

笔记本电脑一台，笔记本电脑此时的优势就突显出来啦！因为它有两张网卡，一张有线网，一张无线网卡，

我这里用有线网卡设医保网 IP，无线网卡设互联网 IP（通过无线路由访问互联网）：

医保网网卡 IP：192.168.10.154 网关：192.168.10.1 子网掩码：255.255.255.0

互联网网卡 IP：192.168.60.21 网关：192.168.60.1 子网掩码：255.255.255.0

具体方法：

点开始 - 运行 - 输入 cmd。

依次输入：

route add 192.168.10.0 mask 255.255.255.0 192.168.10.1

route delete 0.0.0.0

route add 0.0.0.0 mask 0.0.0.0 192.168.60.1

下面看看，ping 192.168.10.1/ping www.baidu.com，网络都是通的吧？

把这些语句放入记事本，另存为 .bat 文件，当我们需要厂商工程师远程协助时，接上内网网线，就可以双击此 bat 文件，然后用 QQ 或其它远程工具对医院内网进行访问。

远程协助完毕后，重启电脑，电脑自动恢复到原来默认状态，不影响使用。

总结一下，这样操作不影响交换机、路由器的任何配置协议，且简单实用。

❖ 4KB 扇区硬盘安装之路

北京 张棋

当服务器装上机架后，作者按照惯例使用戴尔 Lifecycle 程序引导进行 VMware ESXI 6.0 安装。在进入

Lifecycle 程序后，首先配置 RAID，将服务器 3 块 600G SAS 硬盘配置成 RAID 5，空间大小为 1.09T。选择 OS 部署，根据 Lifecycle 程序引导选择开始安装 VMware ESXI 6.0。服务器重启后，进入安装程序，当选中安装程序所找到 RAID 硬盘空间，出现错误提示，并退回到初始的安装界面，并在此过程中反复。

作者认为可能是硬件问题，于是在另一台服务器进行安装，但遇到同样的问题。是不是软件兼容性问题？作者开始尝试安装 Windows Server 2012，安装程序在选择硬盘时，提示“Windows 无法安装到这个磁盘。这台计算机的硬件可能不支持启动到此硬盘。请确保在计算机的 BIOS 菜单中启用了磁盘的控制器”，安装也无法继续。作者开始了漫长的排错，不管是否通过 Lifecycle 进行操作系统安装，VMware ESXI 6.0，Windows Server 2008，还是 Windows Server 2012 都不能正常安装。那怕是将这台服务器的 3 块硬盘装到单位之前改买的同型号的 R730 上，也不能安装操作系统。是不是硬件故障？使用戴尔服务器的硬件检测程序，进行了全面的检测，2 台服务器都没有任何问题。那究竟是什么原因造成？

作者与戴尔售后工程师经过多天的沟通，最终将故障的原因定位到了 3 块硬盘。这 3 块硬盘与同型号 R730 服务器所采用 600G SAS 6Gbps 硬盘不同的是，采用了 600G SAS 12Gbp 原生 4K 扇区的 SAS 硬盘。经查询技术文档，原来为了提高硬盘容量、传输速率和纠错效率方面的，存储设备厂商开始生产 4KB 扇区硬盘。早期，

为了提高 4KB 扇区硬盘的兼容性，物理 4KB 扇区模拟成 512byte 扇区。目前，厂商直接生产了原生 4KB 扇区的硬盘，这种硬盘物理和逻辑扇区字节数都是 4KB。而使用原生 4KB 扇区的硬盘，需要服务器 BIOS/UEFI、存储控制器和操作系统多方面支持，缺一不可。但是目前，并不是所有的操作系统都支持原生 4KB 扇区的硬盘，例如 VMware ESXI 就不支持原生 4K 扇区的硬盘（具体说明可见 <http://kb.vmware.com/kb/2131787>）。Windows Server 系列也仅 Windows Server 2012 支持原生 4K 扇区的硬盘。

那为什么前期安装过程中，Windows Server 2012 也不能正常安装呢？作者在查询微软的技术文档后，发现不能通过常规方式来安装系统。要避免在安装过程出现“我们无法创建新分区。”的问题，需在安装向导进入“要在哪里安装 Windows？”页面时，按 SHIFT+F10 以打开命令提示符。依次输入如下命令：

```
diskpart
select disk 0
clean
convert gpt
```

通过命令将硬盘分区表模式改为 GPT，关闭命令提示符窗口返回到安装向导，就可以继续完成 Windows Server 2012 的安装。

此次操作系统安装过程给作者的经验，不能忽略硬件系统的细小变化，些许变化就可能会造成兼容问题。

❖ 如何延长 UPS 的使用寿命

福建 李贵华 马记

负载数量应适中

很多维护人员习惯将 UPS 接口接满各类设备，以“物尽其用”。但这样会让 UPS 长期处于满载状态，缩短使用寿命。若 UPS 实际应用负载低于额定负载的 30%，内部电池组不能完全正常地工作，也会影响其使用寿命。一般情况下，在线式 UPS 负载量应该控制在 70% ~ 80%。后备式 UPS 应该控制在 60% ~ 70%。

感性负载不搭接

UPS 的负载应为纯电阻负载或电容性负载，而电感性负载，如电风扇、冰箱、空调等，不宜与 UPS 共用一相电路，因为电感性负载的电流往往会超过额定电流的 3 ~ 4 倍，从而引起 UPS 的瞬时超载，影响 UPS 的寿命。UPS 的防磁能力稍差，也不宜将 UPS 靠近强磁性物体。

定期维护是保证

蓄电池组是 UPS 的核心组成部分。多数中小型 UPS 采用免维护密封式铅酸蓄电池, 充电时, 电压过高会造成过量充电, 使电池组鼓胀、变形、漏液甚至破裂。当充电电压不正常的时候, 也会让电池配置数据产生错误。另外, 应每半年测量一次 UPS 的端电压, 如果电压超过 1V, 就应该使用均衡的恒压限流 (0.5A) 充电, 若不奏效只能换新电池。UPS 长期供电时, 应定期中断供电, 让 UPS 带负载放电 3 ~ 5 分钟, 以激活电池。

工作环境要讲究

UPS 的使用环境要求清洁、少尘、干燥, 灰尘和潮湿的环境会引起 UPS 工作不正常。一般要求每两年打开 UPS 机壳, 清洁机内灰尘。而 UPS 的电池组对温度要求较高, 标准使用温度为 25℃, 平时不应超出 15℃ ~ 30℃。另外, 虽然 UPS 中有压敏电阻、热敏电阻、放电管等避雷击器件来吸收谐波和雷击干扰, 但仍要确保 UPS 的有效屏蔽和良好接地, 使防雷设备能发挥较好的作用。

快速破坏环路

福建 王刚 曾玮琳 郑洪飞

为了能够及时发现网络中的二层网络环路, 避免对整个网络造成严重影响, 当网络中出现环路时, 可利用交换机环路检测技术 (Loopback Detection), 及时发出告警信息, 通知用户检查网络连接和配置情况, 并能够将出问题的接口置于某种管制状态, 以实现快速破坏二层网络环路, 最小程度地影响网络使用, 环路检测功能并不能破坏二层网络环路, 必须结合交换机物理接口管制状态才能快速破坏二层网络环路。

二层环路危害

所有环路的形成都是由于目的路径不明确导致混乱而造成的, 环路会造成网络动荡, 引起数据包数量增加, 造成丢包, 严重时会导致网络瘫痪。在多数网络故障中, 链路和设备故障导致网络通讯质量下降的占多数, 通常在网络部署和网络设备调整过程中也会因路径的设置不当导致二层网络环路, 造成各种危害。

环路一旦形成, 网络中的环路会对广播、组播以及未知单播等报文进行不断地循环转发、广播和重复发送, 无法结束进而造成网络广播风暴, 阻塞带宽, 耗尽交换资源, 能让交换机的 CPU 使用率高达 85% 以上, 造成网络资源浪费甚至交换机瘫痪。

由于交换机具有学习功能, 网络内的主机只要发送

广播报, 交换机就必须在相应的物理端口学习 MAC 地址形成 MAC 地址表, 当有环路存在时, 交换机会在多个端口学习到同一 MAC 地址和 IP 地址, 从而形成错误的 MAC 地址表, 这种现象就是 MAC 地址漂移, 会影响数据包的正常转发, 造成网络中断。

二层环路产生原因

在规模较大的局域网网络中, 时常会遇到网络通道被严重堵塞的现象, 造成这种故障现象的原因有很多, 常见的主要原因有 6 种。一是网络中交换机改动、乱入或位置变化。因为频繁改动网络时很容易引发网络环路, 而由网络环路引起的网络堵塞现象常常具有较强的隐蔽性, 不利于故障现象的高效排除。二是网络线路调整。在调试设备时测试光路形成的环路。有时我们会在远端进行线路回环对线路是否正常进行测试, 有时因操作导致线路混乱而产生环路。三是配置不当。例如, 为实现二层网络双路由保护或流量分担, 链路进行聚合操作, 当在参加的接口上取消了链路聚合功能就会形成环路, 还比如, 交换机启动了生成树协议, 当取消生成树协议后, 原来可能阻塞的环路恢复环路等。四是病毒引发环路。原本网络中存在环路, 但因生成树协议后环路失效, 病毒引发线路阻塞, 导致生成树保活的协议失效, 导致

生成树协议失效，引发环路恢复。五是报文转发异常导致环路。当数据转发给外连交换机时，因外连交换机的处理能力不足，外连交换机会反弹转发，从而造成网络环路。六是硬件故障。这种故障比较少，因为即使交换机接口出现故障一般也不会形成环路，但有时接口被高压等原因击穿后接口内部会形成环路。

环路检测原理及报文结构

环路检测技术是通过连续周期性发送环路检测报文来检测网络中是否存在环路的检测技术。二层环路分为单臂环路和双臂环路，单臂环路为环路检测报文从交换机某端口发出，又从该端口接收到该环路检测报文如图 1 所示，可以判断出该接口产生物理故障或外连网络有环路。双臂环路为环路检测报文从交换机端口发出，从该交换机的另一端口接收到环路检测报文，可以判断出该接口产生物理故障或该交换机产生自环如图 2 所示。

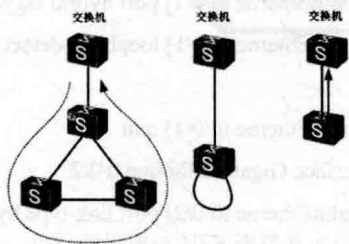


图 1 环路检测报文

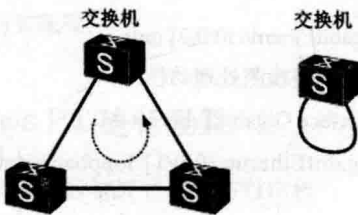


图 2 交换机产生自环

环路检测报文是由交换机发送，报文携带交换机自身 MAC 地址和相应接口的接口信息，目的 MAC 地址为 BPDU MAC、广播或组播，这样就可以区别于其他交换机发出的检测报文，当交换机接口在接收到自己发送的检测报文后会进行比对，如果 MAC 地址是自己的 MAC 地址则说明网络中存在环路，如果报文中的接口信息同接收到报文的接口信息一致，则说明网络中存在单臂环路，如果不一致则说明网络中存在双臂环路。华为交换机环路检测报文结构说明，如表 1 所示。

DMAC	SMAC	Vlan tag	LDT-Type	Port Information	Flag
字段名称		字段含义			
DMAC	目的 MAC 地址，如果是 Tagged 报文，取值为全 F；如果是 Untagged 报文，取值为 BPDU MAC，也可配置为广播或组播 MAC				
SMAC	源 MAC 地址，交换机 MAC 地址				
Vlan tag	默认为 0x8100				
LDT-Type	检测报文的类型，包括协议号和子协议号两部分。其中，协议号取值为 0x9998，子协议号取值为 0x0001，表示是环路检测报文				
Port Information	发送检测报文的接口信息				
Flag	表示 Untagged 报文或 tagged 报文，Untagged 用于普通接口检测，tagged 用于 Vlan 环境检测				

表 1 检测报文结构说明

启动环路检测后，一旦网络中有网络环路，交换机会发送告警和记录日志，并能根据管理员事先设置的处理动作使物理接口处于相应的管制状态，从而快速破坏二层网络环路，减小环路对交换机乃至整个网络的影响，接口被管制后仍会继续发送检测报文，当在设定的时间或默认的时间内再未接收到检测报文后就认为网络中的环路被消除了，这时被管制的物理接口会恢复为正常工作状态。

LDT-Type 检测报文的类型，包括协议号和子协议号两部分。其中，协议号取值为 0x9998，子协议号取值为 0x0001，表示是环路检测报文。

Port Information 发送检测报文的接口信息。

Flag 表示 Untagged 报文或 tagged 报文，Untagged 用于普通接口检测，tagged 用于 VLAN 环境检测。

环路检测功能配置方法（以华为交换机为例）

环路检测配置注意事项

一、环路检测使能后需要发送大量检测报文来进行环路检测，会消耗大量的网络资源，如非排除故障最好关闭环路检测功能。二、因 Eth-Trunk 接口及其成员接口都不支持配置环路检测，不建议和生成树等协议共同使用。三、为减少环路检测报文发送数量和频率，可对发送环路检测报文默认周期适当延长。

配置方法

使能环路检测命令

（1）当交换机未划分 VLAN 时

进入系统视图，在系统视图执行 loopback-detect enable 命令，使能所有接口的环路检测功能。如需在单个接口使能环路检测功能，方法如下：一是在系统视图

执行 interface interface-type interface-number，进入接口视图（interface-type 为接口类型，比如：GigabitEthernet 接口、Vlanif 接口。interface-number 为相应接口或 VLAN 编号，比如：0/0/1、100 等）。二是执行命令 loopback-detect enable，在此接口使用环路检测功能。

（2）当交换机划分 VLAN 时（对指定 VLAN 进行检测）

在系统视图执行 interface interface-type interface-number 命令，进入 VLAN 接口视图。执行命令 loopback-detect packet vlan xxx（xxx 为指定 VLAN 检测编号），配置对指定的 VLAN 进行环路检测。

配置检测报文的发送周期

执行 loopback-detect packet-interval xxx 命令（xxx 为设置的发送周期时间，默认为 5 秒），配置环路检测报文的发送周期。

配置环路检测处理动作

华为交换机环路检测处理动作有 5 种，如表 2 所示。

执行命令 interface interface-type interface-number，进入接口视图。执行命令 loopback-detect action { block | nolearn | shutdown | trap | quitvlan }（默认情况下，环路检测对接口的处理动作为 shutdown）。

动作名称	动作作用
Trap	上报告警并记录日志，但对接口不做任何处理
Block	阻塞接口
No learning	禁止接口 MAC 地址学习
Shutdown	关闭接口
Quitvlan	退出 VLAN

表 2 处理动作

配置事例

如图 3 所示。



图 3 配置事例

配置思路

为检测交换机 A 所在网络是否存在环路，可以在交换机 A 上的 GE0/0/1 和 GE0/0/2 上分别使能环路检测功

能，并配置对 VLAN 100 进行环路检测，实现对交换机 A 所在网络环路检测。

配置步骤

一是使能接口的环路检测功能

```
<Huawei> system-view
```

```
[Huawei] sysname SA
```

```
[SA] interface Gigabit Ethernet 0/0/1
```

```
[SA-Gigabit Ethernet0/0/1] loopback-detect enable
```

```
[SA-Gigabit Ethernet0/0/1] quit
```

```
[SA] interface Gigabit Ethernet 0/0/2
```

```
[SA-Gigabit Ethernet0/0/2] loopback-detect enable
```

```
[SA-Gigabit Ethernet0/0/2] quit
```

二是配置接口对指定 VLAN 报文进行环路检测

```
[SA] vlan 100
```

```
[SA-vlan100] quit
```

```
[SA] interface Gigabit Ethernet 0/0/1
```

```
[SA-Gigabit Ethernet0/0/1] port link-type hybrid
```

```
[SA-Gigabit Ethernet0/0/1] port hybrid tagged vlan 100
```

```
[SA-Gigabit Ethernet0/0/1] loopback-detect packet vlan
```

100

```
[SA-Gigabit Ethernet0/0/1] quit
```

```
[SA] interface Gigabit Ethernet 0/0/2
```

```
[SA-Gigabit Ethernet0/0/2] port link-type hybrid
```

```
[SA-Gigabit Ethernet0/0/2] port hybrid tagged vlan 100
```

```
[SA-Gigabit Ethernet0/0/2] loopback-detect packet vlan
```

100

```
[SA-Gigabit Ethernet0/0/2] quit
```

三是配置环路检测处理动作

```
[SA] interface Gigabit Ethernet 0/0/1
```

```
[SA-Gigabit Ethernet0/0/1] loopback-detect action
```

block

```
[SA-Gigabit Ethernet0/0/1] quit
```

```
[SA] interface Gigabit Ethernet 0/0/2
```

```
[SA-Gigabit Ethernet0/0/2] loopback-detect action
```

block

```
[SA-Gigabit Ethernet0/0/2] quit
```

实验结果

刚配置完毕，在系统视图执行 display loopback-detect 命令，可以看到配置结果如图 4 所示。



图 4 配置结果

再等待一段时间，在系统视图执行 `display loopback-detect` 命令，可以看出接口 `GigabitEthernet 0/0/2` 被阻塞如图 5 所示，二层环路被破坏。



图 5 阻塞示意

破坏交换机 B 和交换机 C 之间的链路，再过一段时间，发现链路中无环路检测报文，说明网络中无环路，如图 6 所示。



图 6 说明

利用交换机环路检测功能，当网络中存在二层网络环路，可以快速发现二层网络环路，通过物理处理动作可快速破坏环路，减少中断时长，最大程度减少损失。

❖ Mac 在 Windows 上的打印

威海 赵永华

办公室有一台打印机通过 USB 连接着一台 Windows 机器，这是一台简单的打印机并没有连通 Internet；你自己用的是 Macbook，有文档想要共享那台打印机，用软件方式如何实现呢？

对 Windows PC 进行配置

进入控制面板后打开“设备与打印机”，鼠标右键点击打印机图标后选择打印机属性；

在打印机属性窗口内，切换到共享栏目后勾选“共享此打印机”，并对其加以标示。

最后，在 Windows 中进入命令行后输入命令“`ipconfig /all`”，然后从 Hostname 处找到该计算机的名称。

配置你的 Mac

在 Mac 机上进入 System Preferences 打开 Printers & Scanners；

点击 + 按钮添加新的打印机，然后切换到 Windows 栏目选择你的工作组，它应当与打印机所连的上述 Windows PC 主机相一致；

从列表中选择共享打印机，然后在 Use 栏目下选择“Select Software”，从列表中选取打印机模式；

点击 Add 按钮，旨在从 Mac 访问此打印机，转到 System Preferences，勾选 Printer Sharing，并勾选“Everyone”和“Can Print”

至此，你在 Mac 上打开需要打印的文本如文字编辑软件，只要按下组合键 `Cmd + P` 就能调出系统打印会话框，然后从可用列表中选择 Windows 打印机即可。

但有时并不顺利，比如出现打印阻塞问题，此时你需要从打印队列中点击你的打印作业，然后输入你在 Windows 中的用户名及密码，然后才能开始打印。但往往还会出问题，下次打印还是需要你输入用户名和密码，但是你在上次输入时，明明已经勾选了“Allow this information to be saved in Keychain on the Mac so it won't have to be entered in the future.”方式，对此如何是好？此时，你可以将此打印机从你的 Mac 列表中删除，

重新执行一遍刚才的配置过程，即重新添加该打印机；另一种方法是在 Mac 上打开 Keychain 访问，搜索到该打印机名称删除输入项，此时发送一个打印作业，输入 guest/guest 作为你的网络审核方式，并保存在 Keychain

当中。或者你就直接转到 Printers & Scanners，右点打印机名称后选择 Reset Printing System，此时就是柳暗花明又一村了。

寻找丢失的交换机

宁波 姚明友

因为业务扩展需要，需在短期内将新造好楼层里的房间电脑接入单位内网使用，但那楼层所需的交换机在我们资产系统上显示已经出库使用，实际却不在新造楼里使用，怀疑是之前临时使用到其它楼层去了，于是翻遍了近日的出借单却都没有找到那台交换机的出借记录。目前手头有该交换机的型号以及序列号的信息，想通过一个个弱电井或机房实地查看，但该方法寻找工作量较大。并且有些弱电井线路拥挤复杂，很难看到交换机的序列号，思索之后想起 Cisco 交换机有查看相邻设备的专属命令：show cdp neighbors，此命令可以查看连接着的相邻设备信息，如图 1 所示。

```
Switch#show cdp neighbors
Capability Codes: R - Router, T - Trans Bridge, B - Source Route Bridge
                  S - Switch, H - Host, I - IGMP, r - Repeater, P - Phone
Device ID Local Intrfce Holdtme Capability Platform Port ID
Switch Fas 0/1 139 S 2960 Fas 0/5
Switch Fas 0/3 139 S 2960 Fas 0/23
Switch Fas 0/7 139 S 2960 Fas 0/24
Switch Fas 0/2 139 S 2960 Fas 0/7
Switch Fas 0/8 139 S 2960 Fas 0/4
Switch Fas 0/4 122 S 2960 Fas 0/1
Switch Fas 0/6 153 S 2960 Fas 0/24
```

图 1 相邻设备信息

通过核心输入此命令开始查找，如果找到对应型号后，使用另外一条命令：show cdp neighbors detail，此命令可以查看相邻设备的具体信息，如管理地址，具体型号等信息，如图 2 所示。

```
Device ID: Switch
Entry address(es):
  IP address : 192.168.1.2
Platform: cisco 2960, Capabilities: Switch
Interface: FastEthernet0/6, Port ID (outgoing port): FastEthernet0/24
Holdtime: 166

Version :
Cisco IOS Software, C2960 Software (C2960-LANBASE-M), Version 12.2(25)FX, RELEASE SOFTWARE (fc1)
Copyright (c) 1986-2005 by Cisco Systems, Inc.
Compiled Wed 12-Oct-05 22:05 by pc_team

advertisement version: 2
Duplex: full
```

图 2 具体型号等信息

查到管理地址后 Telnet 连接交换机，输入命令 show version 查看序列号，如图 3 所示。

```
63488K bytes of flash-simulated non-volatile configuration memory.
Base ethernet MAC Address       : 0060.2F16.9A91
Motherboard assembly number     : 73-9673-09
Power supply part number        : 341-0029-05
Motherboard serial number       : CAT103758VY
Power supply serial number      : DTH1036C7UB
Model revision number           : P0
Motherboard revision number     : A0
Model number                    : WS-C3560-24PS-E
System serial number             : CAT1037E3JF7
Top Assembly Part Number        : 800-26380-04
Top Assembly Revision Number    : B0
Version ID                      : V06
CLEI Code Number                : COM1100ARC
Hardware Board Revision Number  : 0x01
```

图 3 查看序列号

通过查到的序列号与资产出库单上登记的序列号比对，最终找到了那台丢失的交换机。

注意事项：CDP 是 Cisco 设计的专用协议，其他网络设备品牌设备不适用。



批处理实现信息统计

广州 张鹏 谌得志

设计思路

为了满足信息采集需求,批处理程序需要具备采集和传输两方面的功能。信息采集使用系统自带的命令行工具,如 ipconfig、diskpart 等命令实现。采集的信息使用 ftp 进行传输,利用网络中的 ftp 服务器接收各终端上传的结果。

常用命令及实现

硬盘信息的采集

diskpart 是 Windows 下进行硬盘管理的工具,它是一个集成的管理配置环境。在命令行窗口中输入“diskpart”命令,进入如图 1 所示的提示符。在该环境下,可使用若干命令对硬盘进行查看和管理。为了方便批处理程序执行,该工具也支持脚本文件方式执行,采用“diskpart /s 脚本文件”的方式执行。其中“脚本文件”为 diskpart 集成环境的命令集合。由于只需要查看硬盘信息,这里用的 diskpart 命令只包括 list、select 和 detail 三个命令。



图 1 提示符

系统信息的采集

获取操作系统信息可以有多种方法,其中 Systeminfo 命令获取的信息十分丰富,包括操作系统名称、版本、系统型号、处理器及补丁等若干信息,是较为理想的信息采集手段。但是在实际使用过程中,Systeminfo 命令无法正常将扫描的信息存入记录文件中。估计这可能与 Systeminfo 命令的运行方式有关系。由于需要统计信息没有那么详细,于是便采用“wmic os get name”同样可以获得操作系统类型,再使用“ver”获取操作系统的详细版本号。

采集信息的上传

采集信息文件通过 ftp 工具上传到网络中的 ftp 服务器中去。为了方便批处理执行,ftp 工具采用脚本方式执行,其格式为“ftp -s:filename”。其中 filename 为含有若干 ftp 命令集合的脚本。

批处理脚本

写好的脚本如下所示。

```
set /p input= 计算机使用人 :
echo off
hostname >%input%.txt
@echo 开始构造 DISKPART 脚本
echo list disk >t.txt
echo select disk 0 >>t.txt
echo detail disk >>t.txt
echo exit >>t.txt
diskpart /s t.txt >> %input%.txt
@echo 开始获取网络配置
ipconfig/all>>%input%.txt
@echo 开始获取操作系统信息
wmic os get caption >>%input%.txt
ver>>%input%.txt
@echo 开始构造 ftp 的脚本
echo open [ip address]>ftp.tmp
echo [username]>>ftp.tmp
echo [password]>>ftp.tmp
echo dir>>ftp.tmp
echo cd /upload/tem p>>ftp.tmp
echo put %input%.txt>>ftp.tmp
echo bye>>ftp.tmp
@echo 开始上传
ftp -i -s:ftp.tmp
```

@echo 删除生成文件

del ftp.tmp

del t.txt

del %input%.txt

pause

运行后输出结果如图 2 所示，可以看到生成的脚本已经被上传到 ftp 服务器的文件目录之中。

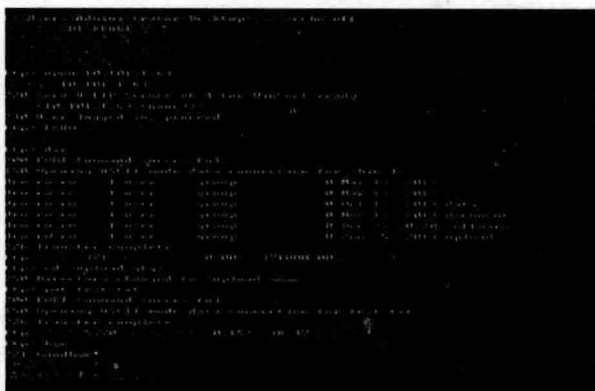


图 2 输出结果

结语

批处理程序是个十分强大的工具集，可以实现丰富了管理功能。采用批处理程序进行计算机信息采集，可以降低终端用户采集信息的难度，降低网管人员的工作量。

◆ 浅谈 ACL 在 SSH 中的应用

山东 何钰 蔡文涓

做为核心路由器，它担负着网络内部横向数据流量和出网纵向流量的高速转发，为了降低设备的安全系数，我们决定将严格限制远程登录设备的用户。目前远程登录设备的方式主要有两种即 ssh 和 telnet。ssh 是安全外壳协议，在登录设备后数据传输的过程中是加密的，而 telnet 方式数据的传输则是明文的，所以我们这次将开启设备的 SSH 功能，并且只允许特定的用户访问核心路由器。如何才能只允许特定的用户访问呢？这里就需要使用 ACL，ACL 即访问控制列表，它可以过滤网络中的流量，是控制访问的一种网络技术手段。下面我们首先定义 ACL 配置命令即：

ipv4-access-list xinzhissh

// 定义一个名称为限制 ssh 的访问控制列表

rule 1 permit 10.66.6 6.0 0.0.0.63

// 规则 1 允许 10.66.6 6.0/26 的网段的 IP 地址

rule 3 permit 10.25 3.140.0 0.0.0.255

// 规则 3 允许 10.25 3.140.0/24 网段的 IP 地址

在 ACL 的条目中我们又定义了允许的 IP 地址段，刚才只是定义了一个 ACL，并没有将该 ACL 应用，所以 ACL 是不起作用的。那么接下来我们将该 ACL 应用到 ssh 中去，配置命令即：

ssh server access-class ipv4 xinzhissh

// 将名称为限制 ssh 的 ACL 应用到 SSH 服务中

ssh server enable

// 使能 SSH 服务

line telnet server disable

// 关闭 telnet 服务

我们将 ACL 应用到了 SSH 中，同时将 SSH 功能也

进行了开启，为了保证设备的安全，我们还关闭了设备的 telnet 服务。这样将最大程度保证设备的安全。通过刚才的配置我们先对 ACL 进行定义，并且将 ACL 应用到了远程登录的 SSH 中，实现了 ACL 在 SSH 中应用，只有匹配该 ACL 条目的流量才能允许登录设备，而其他流量将会被丢弃，最后我们还关闭了设备的 telnet 服务，配置完这些后，尝试使用非 ACL 允许条目中的 IP 地址无论是 telnet 还是 SSH 登录设备都不能成功，这样就说明我们配置是正确的，达到了限制用户登录设备的

目的。其实在网络的日常维护中，作为网络运维人员，思想要开阔，多留意、多考虑网络架构，只有从小的一点一滴的入手，正如不积小流无以成江河是一个道理，正是这样一个不起眼的小措施，才会筑牢我们网络的防火墙，如果说我们放任这些小漏洞，那么这样无疑给网络的安全埋下了一个安全隐患，我们不能杜绝网络安全事件的发生，但是我们要尽量降低网络遭受威胁的系数，从而为网络的健康发展提供坚强的壁垒。

◆ 无线局域网部署的优化

北京 张棋

信息化进程对于现代企业的发展是尤为重要的，而企业信息化的基础是企业网。而企业内部架设的传统的有线网络，在完成初次安装布线后，在移动性、灵活性、可扩充性上面存在严重的不足。无线网络的建设是企业提升信息化发展的必然选择，无线网络具有高度的空间自由性和网络灵活性，有助于简化网络结构，从而增加网络的扩展性。然而，企业在部署自己的无线局域网时，往往因为部署结构、配置不够优化，造成无线资源的浪费。本文将根据实施中遇到的实际情况，提出无线局域网部署中的几种优化方式。

图 1 为本文讨论的无线局域网的网络架构，控制器与 AP 使用同一 Vlan 进行通信。其中，控制器的型号为：Cisco CT5508，控制器使用的软件版本为 8.0。

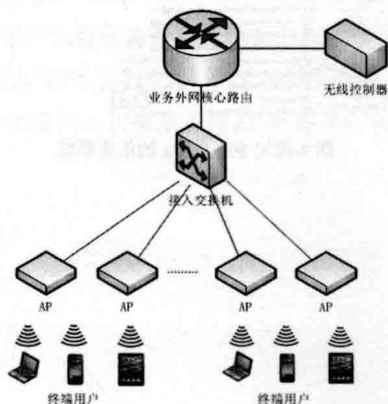


图 1 无线局域网架构

优化方法一

根据实际的物理环境，合理布局 AP 点位，使得每个 AP 可以达到最优的发射功率。Cisco 官方要求两个 AP 之间的间距不小于 8M，考虑到这个因素，在该楼层的 4 个角落各部署一台 AP，部署方式为吸顶挂装。图 2 为某楼层的 AP 部署情况。

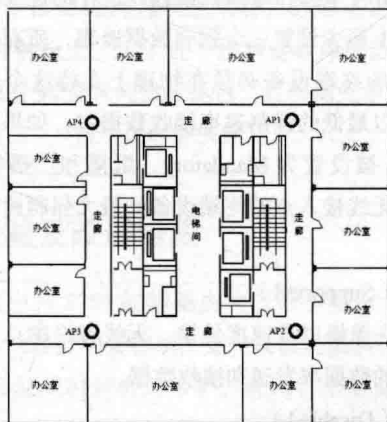


图 2 某楼层布局及 AP 部署位置

部署完成后，需要根据观察到的 AP 发射功率，调整 AP 部署位置；相邻楼层之间，AP 应错位安装，不在同一垂直线上，避免信号相互干扰。

优化方法二

启用控制器的 Band Select 功能，让那些能够支持 5G 的客户端尽量用 5G 的频段来连接 WLAN。

客户端首次连接时, Band Select 就能根据客户端的能力, 在 2.4-GHz 和 5-GHz 这两种频段之间进行分配。在某个 WLAN 上开启 Band Select 功能, 使那些支持 5-GHz 的终端设备固定在该频段上。

优化方法三

根据某 SSID 的用户或应用程序的实际情况, 调整适合的 QoS。QoS 是指网络向一组用户或应用程序提供更好的或特殊服务的能力。

在 802.11e 的修订协议中定义了八个用户优先级 (UP 值), 两个一组, 共分为 4 组, 分别是:

白金 / 语音 (UP 7 和 6) - 确保高品质无线语音服务。

金 / 视频 (UP 5 和 4) - 支持高品质的视频应用。

银 / 尽力而为 (UP 3 和 2) - 支持正常带宽的客户端, 这是默认设置。

铜 / 背景 (UP 1 和 0) - 为访客服务提供最低带宽。

在实际应用中, 可以针对某个 SSID 面向的用户或者应用, 调整该 SSID 的 QoS 级别, 使其性能更优, 用户体验更好。

优化方法四

调整 802.11 b/g/n 的参数, 关闭一些低速率的频段, 以降低信道利用率指数。

对于 Data Rates 这个参数, 有三种选择, 分别是 Mandatory、Supported、Disabled。

强制 (Mandatory)

允许所有单播和组播数据包以这样的速度传输。无线接入点上至少设置一个强制数据速率, 所有关联到无线接入点的终端设备必须在物理上支持这个速率, 并且必须能以最低的强制速率接收数据包。如果不止一个 Data Rates 被设置为 Mandatory, 组播和广播帧会以所有关联到无线接入点的终端设备的最大强制速率进行转发。

支持 (Supported)

只允许单播以该速度传输。无线客户端总是试图在尽可能高的数据率发送和接收数据。

禁用 (Disabled)

无线接入点在该速率不发送数据。

禁用低速率频段, 如: 1Mbps、2Mbps、5.5 Mbps、

6 Mbps, 可以有效地降低信道利用率指数。当然, 关联到无线接入点的终端设备必须支持那些未被禁用的 Data Rates, 否则终端设备就无法接入无线网络。

优化方法五

调整 802.11 a/n 的信道分配, 虽然在 2.4GHz 中 802.11n 被限制使用 20 MHz 信道, 但是在 5 GHz 中可以使用 20 MHz 和 40 MHz。考虑实际需求, 调整信道分配, 如: 高密度部署的环境下使用 20 MHz 信道, 在客户端需要大带宽 (例如视频应用) 时使用 40 MHz 信道。

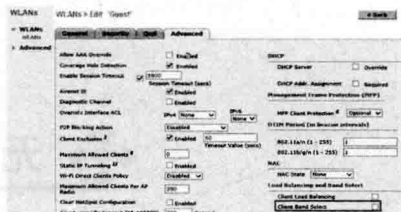


图 3 开启控制器的 Band Select 功能

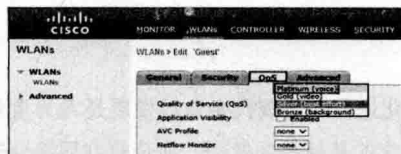


图 4 选择合适的 Qos

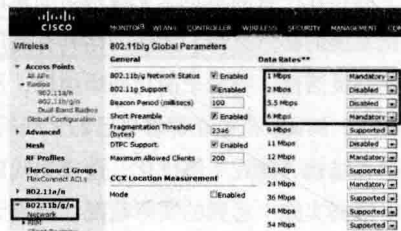


图 5 关闭低速率频段

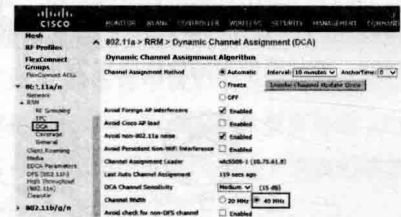


图 6 固定 802.11 a/n 的信道带宽



交叉板故障处理及分析

▼ 新疆 张景 李剑波 热比古丽

网络拓扑

本单位光通信网络由中兴 S385 组成。该网络有 2 个两纤双向复用段保护环，D 站作为两个环的相切点。根据业务走向，A 站作为核心节点，至 B、C、D、E、F 站点均有大量数据和 TDM 业务。

故障经过

某日下午，在开通 A 站至 D 站业务时，业务时隙下发失败，出现“设置网元净荷时隙子网保护，命令执行超时，增量下发失败，可尝试全量下发，但全量下发有可能影响现有业务”告警。尝试再次下发时，仍出现上述告警，这时 A、B、C、D、E、F 站点千兆板出现“帧定位丢失”、“VCG 组丢失”、“AU4 告警指示信号(AIS)”、“背板帧失步”、“VC4 不可用秒开始(UAS)”“VCG 端口宿端丢失全部容量”等告警，A 站点 TGSA 千兆板承载业务全部中断，网管查询不到该板光功率。

故障处理

经中断业务现象分析，中断的业务均由 A 站 S385 千兆板到各方向的业务，拔插克拉玛依站千兆板仍无法恢复千兆业务。

由告警信息判断是交叉时钟板出现了故障，网管上查询 A 站点 S385 运行于 8# 交叉时钟板，于是将 8# 交叉板进行硬复位，切换至备用的 9# 交叉时钟板，在切

换过程中，A 站至各个方向的其他业务也都出现了中断现象，光板、千兆板都同时出现告警，告警数量达到千余条。

初步判断是 9# 交叉时钟板出现了故障后，网管上尝试将交叉时钟板切回 8# 交叉时钟板，业务仍然没有恢复。

这时在网管上将交叉模块切换到清除状态，保证 2 块交叉时钟板的自动主备用切换功能，设备上观察 8#、9# 交叉时钟板，在将交叉模块更改为清除状态时，9# 交叉时钟板运行灯闪了一下后切到了 8# 交叉时钟板上，这时告警逐渐消失，业务逐渐得以恢复。

在将 A 站的 9# 交叉时钟板拔出完成后，继续下业务时下发成功。

故障分析

从以上故障处理过程中来看，故障点定位在 A 站 9# 交叉时钟板上，为了进一步判定故障原因，将 A 站替换下来的 9# 交叉时钟板返修，经检测此单板“上电 - 供电无输出”，“业务 - 时钟失锁”。

维护经验及改进措施

此次中兴 S385 故障是由交叉时钟板故障触发的，因此日常的维护中要特别注意交叉板的散热，加强对于 S385 设备交叉时钟板的维护。在网管上对交叉模块切换后，将交叉板时钟板切至“清除状态”。



浅析高校无线网络的部署

北京 池新杰

随着高校信息化建设的发展,更多的像“数字APP”、“校园微信群”、“MOOC课堂”等要求方便、快速、移动式的网络应用出现,使得传统的有线网络已经很难在满足校园网用户的使用需求。同时,随着移动终端、笔记本电脑等无线局域网客户端适配器产品成为了学生、老师们的“标配”。很多高校开始思考需要建设一套可靠、完善的无线校园网络来满足校园网用户的用网需求,这种无线网络不应该是传统上的辅助型的无线局域网,而是需要具有更大的应用范围,更稳定的性能,更高的访问速度,更灵活部署方式的园区性无线网络。于是很多高校在近几年的无线实验网的探索之后,纷纷开始规划并建设作为有线网络之补充的校园级无线网络,为校区提供全部的无线区域网的信号覆盖,并提供数据接入业务,让学校师生体会到无线局域网给教师的教学和学生的学习带来的好处。

高校无线网络的需求分析

完善的项目部署方案离不开充分的需求分析,在建设和部署一个现代化高校无线校园网之前,我们应当详细的分析高校信息化应用以及校园网用户对于无线网络的使用需求。结合我校无线校园网的建设经验,我总结了以下5种高校无线网络需要满足的条件。

网络架构需求

在网络架构的设计上应结合校园网的实际情况,如果是新建无线网络应该独立于现有的有线网络,也就是形成有线、无线两套物理独立网络,两套网在物理链路上隔离,只在核心设备上建立通信联系。这样做的好处在于可以保证新建无线校园网是一个稳定可靠、可扩展的独立网络结构,为今后以无线网络为主的校园网发展打好坚实的基础。

同时,在无线网络技术上应选择集中式管理方式,即无线控制服务器+无线AP的架构,无线AP通过校

园网的接入层POE交换机设备接入到校园网中。通过无线控制服务器将所有的无线AP进行统一的控制和管理,增强整个无线校园网络的可管理性。

信号覆盖方式需求

高校校园是由不同的区域组成,以我校为例,整个校园分为两大区域:教学区和生活区,其中教学区主要包括教学楼、行政楼、图书馆、实验楼等为师生教学服务的辖区,而生活区则包括宿舍、食堂、体育场馆等为师生生活提供服务的场所。不同区域的无线网络需求也是不同的,这些不同包括无线网络使用的时间,建筑的结构以及用户的密集程度。因为这种需求上的区别,对于无线网络在信号覆盖方式上的要求也是不同的,如:图书馆、会议室在无线网络的信号覆盖范围以及技术选择上肯定要区别于宿舍楼。这些因素是我们在建设无线校园网之前要考虑清楚的。

安全性需求

安全性是网络建设上非常重要的需求,无线校园网具有使用便捷灵活、易于扩展等有线网络无法比拟的优点,但是由于无线网络的信道开放的特点,使得攻击者能够很容易的进行窃听,恶意修改并转发,因此安全性成为阻碍无线校园网发展的重要因素。虽然一方面对无线局域网需求不断增长,但同时也让许多高校用户对不能够得到可靠的安全保护而对最终是否采用无线局域网系统犹豫不决。

在建设无线校园网之前我们要充分考虑到网络的安全。若原有有线网络系统已经具备多种安全防御能力,建成的无线网络首先必须融合进原有网络安全解决方案体系中,并根据无线网络的安全技术特征,补充为具有多层次的安全保护措施,以满足用户身份鉴别、访问控制、可稽核性和保密性等要求。

为了阻止非授权用户访问无线网络,以及防止对无线局域网数据流的非法侦听,无线网络要具有相应的安全手段,主要包括:服务区标识符(SSID)匹配、有线

等效保密 (WEP)、二层隔离、WPA 支持、流氓 AP 的鉴别和防护等。

访问速度需求

如今的高校校园网应用囊括了视频会议、视频点播、VOIP、MOOC 等高带宽应用业务, 这些应用需要用户具备更高的网络带宽和访问速度。在无线网络的建设工程中, 我们要考虑网络访问速度的需求, 选择最为先进且可扩展的无线网络技术, 以满足校园网今后在高带宽应用上的需求。

与认证计费系统融合需求

很多高校都有稳定运行的入网认证计费系统, 在新建的无线网络中, 作为网络接入层的有效补充, 必须考虑完全融合进原有认证计费体系, 支持全网对每一个用户的上网控制、认证与计费的持续运营; 同时还要支持不同的认证计费方式, 如 802.1X 认证方式、WEB-Portal 认证方式等常见的认证技术。

对于计费的策略, 新建无线网络可以和有线统一融合, 在同一个账户下缴费, 既能为师生提供有线、无线接入的差异化服务, 有利于日后有线、无线校园网的维护管理。

高校无线网络的部署策略

充分了解了高校校园网的需求分析后, 便可以规划详细的无线校园网部署方案, 以下是根据我校无线校园网工程实际规划案例。

网络结构设计

整个无线网络采用扁平化的部署策略, 分为核心层、接入层和无线覆盖层三部分。

无线控制服务器 (AC) 作为所有无线发射端 (AP) 集中控制单元, 通过万兆链路连接到核心交换机上; 作为 AP 接入设备以及供电单元的 POE 交换机分布安放在各个楼宇弱电间, 并通过万兆链路上联到核心交换机; AP 作为无线网络信号发射单元, 通过不同频段发射无线信号, 为用户无线终端提供接入途径。

无线数据转发方式

大规模建设无线校园网必然要考虑无线数据转发的问题。无线数据有两种转发方式:

集中转发, 无线 AP 与无线 AC 通过 CAPWAP 建立隧道, 将无线数据在隧道中封装, 将 802.11 的无线数据封装后, 转发到 AC 上, AC 经过 802.11 到 802.3 数据包转换, 转换为可以在以太网中传输的数据帧格式。

分布转发, 无线 AP 根据数据包的 SSID 和 VLAN 等信息, 自动区分数据包, 在 AP 本地进行 802.11 到 802.3 的数据包的转发, 特定 SSID 的数据不再经过 AC 统一集中转发。

这两种转发方式有着不同的应用场景, 针对视音频等需要低延迟转发的数据, 可以采用分布式的转发, 无线数据可以就近从接入交换机上转发, 而不用必须经过 AC 集中转发, 尤其是在 802.11n 的大容量的接入数据应用上, 分布式的转发具有更高的处理性能。

针对高安全性的数据建议采用集中式的转发, 例如学校的办公系统、无线视频监控、无线一卡通、教职员工、特殊教师等数据, 必须要上传到 AC, 有 AC 进行安全验证后, 才可正常转发。

无线覆盖方式

为保证无线网络可用性与稳定性, 无线信号覆盖区域信号强度应不低于 -80dBm, 信噪比 $SNR \geq 20$ 。业务使用较为集中区域的接入速率应不低于 140Mbps。

在之前的需求分析已经提到, 不同区域的无线覆盖需求也是不同的, 例如我校的会议室、教室、图书馆、体育馆等空旷区域, 由于空间比较宽阔, 有利于信号的传播, 所以可以选用传统的放装式 AP 部署方案, 即将 AP 安装在室内固定的位置上, 直接发射信号覆盖整个房间。

但是, 在办公楼、宿舍楼等房间密集, 且用户集中的区域, 选择放装式的部署方案就会出现問題, 如按房间放置 AP 则会造成 AP 间的信道串扰, 若在楼道内放置 AP 又会造成无线信号覆盖不均匀。所以针对房间密集的区域, 我们选择的是智分式的无线部署方案, 即每个 AP 通过智分天线引至固定数量房间, 从而减少 AP 的数量, 同时有保证了每个房间的信号覆盖强度一致。

我们将 AP 安装在楼道内, 每个 AP 分出 4 条馈线至 4 个房间, 保证 4 个房间相同的信号强度。同时, 按每个房间 6 个用户计算, 每个 AP 的连接人数不会超过 30 人的负载上限。

无线校园网的安全设计

基于无线校园的集中常见安全问题, 在建设无线校园网时应综合考虑无线安全技术, 在无线网络的各个环节进行相应的安全保护、数据加密、身份认证等安全手段, 实现全方位无线安全防护体系。我校无线校园网的安全策略如表 1 所示。

表 1 无线校园网安全策略

类别	采用安全技术	解决的问题
物理接入	WEP64/128、TKIP、CCMP 加密 可升级支持 WAPI 加密	防止无线报文被监听和篡改
	SSID 隐藏	解决不明用户访问
逻辑链路	PSK/MAC/Portal 多种认证方式的混合接入	用户身份鉴别和安全准入
	动态下发用户的权限	业务隔离
	Hotspot 用户隔离	限制用户互访
	黑名单	限制恶意用户
网络	无线入侵检测系统	非法设备的检测、无线攻击的告警和规避
	下行流量限速	避免在大量的无线接入点部署策略
	安全策略在无线控制器统一部署	防范外界对 AP 的数据流量攻击
	AC 和 AP 间的 CAPWAP 隧道下行流量限速	端到端的安全加密
	IPSEC VPN	信息的绑定 (MAC、ESS、VLAN、Port)
设备	AP 本地不再保存配置信息	尽可能防止假冒
	AP 身份认证	避免设备丢失造成配置泄漏
	AP 支持多无线控制器的冗余备份	只有合法的 AP 才能和无线控制器建立关联
网管	无线安全策略配置	无线控制器 down 机不会造成无线网络的瘫痪
		无线安全策略的统一部署

结语

随着教育信息化以及互联网技术的快速发展，高校的基础网络建设必将迎来革命性的发展，而无线网络会成为未来高校网络建设的重中之重。只有充分理解无线网络建设的目的与意义，采用先进成熟且最为合适的部署方案，有的放矢，才能建设成一套稳定、高效、安全、先进的校园无线网络。

双绞线系统中问题的解决

北京 薛仑

近期，笔者在一次综合布线项目的双绞线系统中，遇到这样一个状况：非屏蔽双绞线从设备间到桌面敷设完，信息模块打线完毕后，使用普通的连通性测试仪测试，所有双绞线从桌面信息模块到设备间配线架，均线路通畅，线序正确。但项目验收需要使用福禄克电缆认证分析仪测试通过。在验收过程中出现有近 10% 的信息点无法测试通过，原因均为近端串扰（“NEXT”）测试项无法通过。

什么是近端串扰

串扰

串扰是指两条信号线之间的耦合、信号线之间的互

感和互容引起线上的噪声。

近端串扰

近端串扰（Near End Cross-Talk (NEXT)）也叫近端串音，是指在非屏蔽双绞线电缆链路中一对线与另一对线之间的因信号耦合效应而产生的串扰，是对性能评价的最主要指标，近端串扰用分贝来度量，分贝值越高，线路性能就越好，有时它也被称为线对间 NEXT。

近端串扰过大的原因

众所周知，综合布线中常用的双绞线为 4 对相互绞绞在一起的绝缘铜线组合在一起。为了降低信号的干扰程度，双绞线中的每一对双绞线一般是由两根绝缘铜导

线相互扭绞而成，双绞线也因此而得名。双绞线又分为屏蔽双绞线和非屏蔽双绞线。屏蔽双绞线由于每对绞线都带有屏蔽层，基本可以规避近端串扰。在非屏蔽双绞线中减小线对之间的串扰即近端串扰的主要手段就是线缆中的绞结。质量好的双绞线每对线缆的组合比较密，扭距比较小。

在非屏蔽双绞线系统中如果破坏绞结过多或绞距遭到破坏，都有可能导致近端串扰过大。当然，所使用的中间连接器——信息模块是否达标也可能对近端串扰的大小有所影响。

因此，综上所述，在双绞线系统中非屏蔽双绞线近端串扰过大（即电缆认证分析仪测试，“NEXT”项测试无法通过）主要有三个原因：

- （1）双绞线的质量未达标；
- （2）信息模块质量未达标；
- （3）布线施工时工艺高低。

近端串扰过大的影响

由近端串扰的定义我们便可以知道，它是一种噪音。当噪音过大时，必然会影响链路上的数据传输，轻者降低网速，重者频繁丢包，甚至网络中断。因此，近端串扰是决定网络链路传输性能的一个非常重要指标。

我们用于数据传输并具有检测标准的非屏蔽双绞线主要有2类（CAT 2）、3类（CAT 3）、4类（CAT 4）、5类（CAT 5）、超5类（CAT 5e）和6类（CAT 6）四种。这6种双绞线均可用于语音传输，但在数据传输中随着标准提高，速率也升高。CAT 2线仅可用于最高传输速率4Mbps的数据传输。CAT 3线可用于最高传输速率为10Mbps的数据传输主要用于10BASE-T。CAT 4线可用于最高传输速率16Mbps（指的是16Mbit/s令牌环）的数据传输。CAT 5线可用于语音传输和最高传输速率为100Mbps的数据传输，主要用于100BASE-T和10BASE-T网络。CAT 5e主要用于千兆以太网。CAT 6传输性能远远高于CAT 5e，最适用于传输速率高于1Gbps的应用。

随着非屏蔽双绞线标准及传输速率的提高，相应标准的链路对近端串扰的要求也就越来越高。换句话说，使用CAT 5的双绞线、水晶头和信息模块并不能保证网络链路就一定支持速率100Mbit/s的传输。如果近端串扰过大，有可能只能保证10Mbit/s的速率。我们在实际中也常遇到这样的状况：在部署网络终端设备时，设备

无法正常使用。使用测线器测试链路，线路通畅，线序正确，但是终端设备不是网不通就是丢包严重。有时将设备网卡速率降至10Mbit/s甚至于更换网络跳线，终端设备便可正常使用。这都有可能是整个链路的近端串扰过大造成的。

解决近端串扰过大需要注意的方面

近端串扰过大严重影响网络链路性能。减小网络中近端串扰的主要需注意以下5个方面：

选择质量合格的双绞线

双绞线的质量是影响双绞线系统中近端串扰值的最大要素。不同线对具有不同的扭绞长度，一般地说，扭绞长度在38.1mm至14cm内，按逆时针方向扭绞。相邻线对的扭绞长度在12.7mm以上，一般扭绞的越密其抗干扰能力就越强，近端串扰也就越小。常用的双绞线国外品牌有安普、西蒙、朗讯等，国内品牌有爱讯通、TCL、长飞等。

选择质量合格、规格匹配的信息模块

信息模块在整个双绞线系统中属于中间连接器。如果中间连接器质量不过关，也有可能导致双绞线线对短路，造成近端串扰过大。当双绞线和信息模块规格不匹配，例如CAT 6双绞线采用CAT 5类信息模块也有可能造成近端串扰过大，降低链路性能，达不到CAT 6标准。

提高布线施工标准

布线施工工艺是造成近端串扰过大的最常见的原因。一般地说，双绞线内线对的扭绞长度在13mm以内，因此，在实际施工时，信息模块处绞对打开也不得超过13mm。另外，双绞线的牵引力也不可过大，避免破坏双绞线的绞距。

选择质量合格的网络跳线

双绞线系统验收通过，符合标准，但是由于双绞线跳线的质量不过关，也可能造成网络链路的近端串扰过大，一样可能导致整个网络链路性能的下降或不可用。

布线施工后务必采用电缆认证分析仪进行测试验收。电缆认证分析仪不仅可以测试整个网络链路的连通性、线序，还可以测试衰减、串扰、延迟、电阻等多项影响网络性能的参数。它可以较为准确地评估整个双绞线链路的性能，为我们的验收或者维修提供数据参考。

结语

文中,笔者在综合布线项目中双绞线系统验收过程中遇到的状况,就是因为施工人员在打线信息模块的时

候没有保证信息模块处打开绞对不超过 13mm 而造成。希望大家引以为戒。

解决网络规划中的问题

北京 荆波 河北 王春海

某政务中心 Internet 网络接入规划问题

某政务服务中心,采用 100M 联通、100M 广电专线接入 Internet。广电与联通通过华为 AR-2811 路由器接入,之后连接到一台“联想网御防火墙”,在联想网御防火墙再接局域网核心交换机,连接各上网的工作站,同时联想网御防火墙的 FE5 口接一台“金电网安防火墙”,再接一个普通的交换机(称为“WWW 服务器交换机”),这个交换机连接网站服务器。该网站服务器域名对外的 IP 地址是 y1.y2.251.132,该地址是通过 AR-2811 映射给“联想网御防火墙”,再映射给连接到“WWW 服务器交换机”中的一台 IP 地址为 192.168.60.3 的服务器中。

用户现在存在的问题是:每过一段时间,单位上网比较慢(过一段时间恢复,但网络速度慢的时间不固定),此时 Internet 用户打开单位网站也特别慢甚至不能打开。近期上级要求,政府对外门户网站要能 24 小时对外提供服务。用户的需求是:首先解决访问外网慢时,门户网站外面(指 Internet 用户)不能访问问题,其次解决访问外网慢问题。因为在网络访问慢的时候,与联通公司联系,已经确认不是线路问题(网站的域名 IP 使用联通的线路)。

对于用户提出的要求,并与用户沟通,达成一致意见:用户网站与内部计算机访问 Internet 线路“分开”,为网站保留至少 10M 的带宽。内部计算机上网慢,通过在网络中加装“流量控制”设备来实现。在我们这个案例中,介绍将线路分开,并为网站服务器单独设计出口的问题。

你可能注意到,联通线路的出口 IP 地址是

y1.y2.251.166,子网掩码 255.255.255.252,上联口(对端,联通的设备地址是)y1.y2.251.165。而 Web 服务器使用的是 y1.y2.251.132 的地址。而 y1.y2.251.132/28 与 y1.y2.251.166/30 并不是同一子网的地址。另外,在查看华为 2811 路由器的配置,看到映射的公网地址是 y1.y2.251.131 ~ 140 的 IP 地址,实际上是使用了 y1.y2.251.130/28 的整个子网。

另外,经过与联通公司查询,该单位还使用了 y1.y2.249.240/30 的地址。但经过对比服务器的设置,发这一地址段也已经不用。为什么设置了这么多段地址呢?因为在前几年,该中心对外的服务器数量较多,而每个服务器都需要一个公网的 IP 地址,并且用户的 IP 地址需求是慢慢增加的。而在以前“传统”的分法中,一般都是给专线用户一段连续的地址,子网掩码是 255.255.255.252(用户只有一个可用 IP 地址)或 255.255.255.248(8 个地址,可用地址 5 个)或 255.255.255.240(16 个地址,可用地址 13 个)。这样就造成了,在规划好后,当用户再需要 IP 地址时,没有办法添加,所以联通公司,专门给该单位添加了一条静态路由,专门设置了 y1.y2.251.164/30 的一段“互联互通”地址,为用户添加了两个可用的子网 y1.y2.251.130/28 及 y1.y2.249.240/30 两段地址,可以使用 20 个 IP 地址(16+4)。但这样造成的浪费也比较大。

此时,如果要在计算机上使用其他的公网地址,需要再在 GE1 口,添加第二个 IP 地址,例如,要使用 y1.y2.251.130/28,需要在 GE1 接口上添加 y1.y2.251.129 的子地址。

ip address y1.y2.251.1 66 255.255.255.252

ip address y1.y2.251.1 29 255.255.255.240 sub

这样,从服务器到联通机房,就多过了一级设备(路由器)。即通过联通公司→华为 2811 路由器,再通过华为 2811 路由器的 GE1 端口接一个交换机,分成两条线,分别为内部计算机提供 Internet 接入,及为 Web 服务器提供专线。这要华为 2811 即是一个“公共”的接点。而如果想让服务器“直接”到联通机房,则不能实现。

所以,为了解决这个问题,在查询到 y1.y2.249.240/30 地址不用的情况下,联系了联通机房,让联通更改级联地址,取消 y1.y2.251.165 的地址,改为 y1.y2.251.142,在路由器上,将默认路由的出口地址由 y1.y2.251.165 改为 y1.y2.251.142(内网计算机访问 Internet 的出口 IP 地址),将原来 Web 服务器 IP 地址从华为 2811 中的映射去掉,改为设置在新添加的软件防火墙 Forefront TMG 的外网上,此时网络拓扑改为图 1。

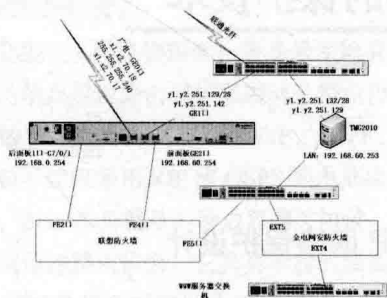


图1改进后的网络拓扑

改进后,联通光纤(通过光电收发器转为 RJ45 接口)先接到一个交换机上,在该交换机上再通过两条 RJ45 网线分别接华为 AR2811 及新添加的一台安装 Forefront TMG 的服务器的“外部网卡”,而 Forefront TMG 服务器的另一块网卡(命名为“内部网卡”)连接到另一台新添加的普通交换机上,此普通交换机再连接原来联想网御防火墙的 FE5 口及金电网安防火墙的 EXT5 端口。此时“WWW 服务器交换机”中,各个 Web 服务器的网关地址由原来的 192.168.60.254 改为 192.168.60.253,并在每台 Web 服务器中,添加到局域网其他网段的静态路由:。

```
route add p 192.168.0.0 mask 255.255.0.0 192.168.60.254
```

在新添加的 Forefront TMG,使用“Web 服务器发布规划”,使用主机头名(即类似 www.abc.net、xyz.com 之类的名称)的方式,发布每个网站到内网中每台服务器的 IP 地址。

【说明】大多数的硬件防火墙、路由器,只能做端口一对一的映射,不能做到端口的“复用”。而 Forefront

TMG 的防火墙,可以用“主机头名”的方式,在只使用一个端口(例如 TCP 的 80 端口或其他端口),根据网站对外域名的不同,发布到内部不同 IP 地址的服务器。这样,在原来需要多个公网 IP 地址时,使用 Forefront TMG,只需要一个公网 IP 地址即可(当然也可以使用多个 IP 地址)。

某单位通过 VPN 网络之后路由器信息没有更新

某单位接入上级政务内网,之后该单位又为其下级单位,依托联通公司,通过联通公司专线使用 VPN 技术组建了内网。

该单位计算机设置 x1.x3.0.1 ~ 250 的地址,子网掩码 255.255.255.0,网关设置为 x1.x3.0.254。该单位其他部门通过 IDC 机房组建 VPN 网络,相关 IP 地址是 x1.x3.10.0 ~ x1.x3.47.0/24。在联通 IDC 机房有一台 x1.x3.120.1 的服务器,该单位及其使用 VPN 的相关部门要访问该服务器。组建之后,每过一段时间,该单位访问上级政府内网出问题,只有重启到上级内网的路由器才能解决,而访问放置在联通 IDC 机房的服务器则无问题。

经过相看 AR 1220 的配置,发现在该路由器中,有如下配置:

```
0.0.0.0 0.0.0.0 x1.x 2.1.9
x1.x3.10.0 255.255.25 5.0 x1.x3.0.253
x1.x3.11.0 255.255.25 5.0 x1.x3.0.253
x1.x3.12.0 255.255.25 2.0 x1.x3.0.253
x1.x3.16.0 255.255.24 0.0 x1.x3.0.253
x1.x3.32.0 255.255.24 0.0 x1.x3.0.253
x1.x3.120.0 255.255.25 5.0 x1.x3.0.253
```

这表示,在访问上级政务内网时,通过 AR 1220 的 GE0 端口及专线访问,而在访问 x1.x3.120.1 及 x1.x3.10.0 ~ x1.x3.47.0/24 网络时,是通过到联通 IDC 机房的专线访问的。这样,所有的工作站在访问 x1.x3.120.1 时,先访问其网关 x1.x3.0.254 即 AR1220 的 GE1 端口,再通过 GE1“转到”IDC 机房的 x1.x3.0.253 线路访问,此其一。如果要解决这个问题,将图 1-3 中的交换机,换为三层交换机,在该三层交换机中规划一个 VLAN,例如 VLAN1001,设置 VLAN1001 的地址是 x1.x3.0.252,在该三层交换机上添加静态路由:

```
ip route-static 0.0.0.0 0.0.0.0 x1.x3.0.254
```



```
ip route-static x1.x 3.10.0 255.255.255.0 x1.x 3.0.253
ip route-static x1.x 3.11.0 255.255.255.0 x1.x 3.0.253
ip route-static x1.x 3.12.0 255.255.252.0 x1.x 3.0.253
ip route-static x1.x 3.16.0 255.255.240.0 x1.x 3.0.253
ip route-static x1.x 3.32.0 255.255.240.0 x1.x 3.0.253
ip route-static x1.x 3.120.0 255.255.255.0 x1.x 3.0.253
```

之后，修改该单位每台计算机的网关地址为 x1.x.3.0.252，这样，在计算机访问 x1.x.3.120.0 及 VPN 网段时，通过交换机的静态路由配置，是访问 x1.x.3.0.253；而访问上级网络则是通过 x1.x.3.0.254 访问。

另外，在查看 AR1220 的配置时，发现其 GE1 的 IP 地址是 x1.x.3.0.254，但子网掩码是 255.255.128.0，这存在设置错误问题，此问题的原因是：原来在没有通过联通 IDC 组建 VPN 网络时，该单位的地址是 x1.x.3.0.0 ~ x1.x.3.127.0/24，故子网掩码设置为 255.255.128.0 不存在问题（原来也没有三层交换机，是直接设置一大段 IP 地址）。但后来组建 VPN 之后，x1.x.3.0.0/24 单独分配给该单位机关使用，此时就不能再设置 255.255.128.0 的子网掩码了，需要将其修改为 255.255.255.0。

企业外包呼叫中心的保护技术

江苏 吴佳成

呼叫中心在企业应用中已经逐渐从电话营销中心向着 CTI（计算机通信集成）综合呼叫中心转变，已经将电话、计算机、互联网等多种媒介综合应用于营销、服务等多项工作当中，它在企业中的位置也是越来越重要。而建立一个规模化的呼叫中心在成本、技术、维护各方面对中小型企业都是一个不小的挑战。

项目背景

某房地产企业通过了解准备利用 ISP 的核心网络 NGCC 成立自己的呼叫中心，通过相互沟通，客户提出了如下基本要求：满足 200 个左右话务台的接入，7×24 小时服务，不能有 1 小时以上大面积断网。考虑到本类型的呼叫中心核心业务实现和控制均在 ISP 核心网内部（已经有充分的网络保护和快速回复能力），所以根据企业对业务的安全和稳定性要求，我们在设计和实施时主要考虑的是在本地网络的保护上，首先由于中心业务能力实现全部在核心网，对接入带宽要求较高，且中心机房为了节省成本建设在郊区乡镇上，肯定要通过单模光纤接入才能满足要求，内部网络在同建筑楼内可以采用网线或者多模光纤互联。下面对网络的不同部分分别采用不同的保护技术及其设计过程做一个详细讨论。

接入 ISP 网络保护设计

考虑方案一：光纤接入由于现代城市施工、外力影响、ISP 割接等导致光缆纤芯中断概率较高，需要考虑采用双光路接入，两条光路走不同的物理路由，保证单路由中断不影响另一路数据传输。物理冷备份有了，业务的自动切换保护技术可以采用 RSTP（快速生成树协议）或者以太网链路聚合（可选静态捆绑或者动态 LACP 协议聚合）。

RSTP 技术优点成熟简单，任何现代交换机路由器都支持，缺点是协议要完全阻断一条备用链路，链路利用率低。以太网聚合也非常成熟，同时两条链路能实现负载均衡。两种技术保护和切换时间均能符合客户要求。但是本方案存在共同的缺点就是都只保护了链路，任何一端设备出现故障或者 ISP 设备升级均会导致全网中断，并且处理故障时间都不能满足企业的要求。

考虑方案二：既然单设备不能满足要求，就在以上双路由基础上再采取 1+1 设备的保护。

客户端两台路由器分别接入 ISP 不同局点的两台路由器，实现异地双设备接入和双链路的硬件备份保护，任何单台硬件系统升级或设备损坏都能得到有效保护。由于拓扑结构的变化，以上的业务保护技术已经不能实现，一般在不同企业之间互联首选的是静态路由方式。

所谓静态就是客户端分别用静态默认路由指向 ISP，针对客户的 IP 段，在 ISP 两侧路由器上分别指向客户本地路由器的互联地址，同时发布进 ISP 对应呼叫中心网络的 VPN 动态路由之中，这样网络就能双向互通，优点是对路由器性能要求较低、维护配置简单，缺点是静态路由感知能力较差，只有在接口 down 时路由器才会自动删除该路由。面对 WAN 接入中复杂的故障情况有点力不从心。比如：当对端设备出现软件故障无法转发数据时，本端路由器无法感知继续转发导致数据全部丢失；当光纤链路出现单芯中断（两端设备又没有启用接口自协商功能，不同厂家设备互联一般不建议采用自协商）时导致一端接口 down 一端 up 的情况，那么在 up 端路由器中该静态路由依然安装在路由表中，也会导致数据全部丢失。此时虽然另一链路完全正常，也会造成网络中断或时断时续。

考虑方案三：网络物理架构还是采用原有架构，针对方案二的缺点逻辑路由保护采用动态路由协议。现在流行通用的动态路由协议主要有 RIP、OSPF、BGP 等，而 ISP 一般不建议采用 RIP 或 OSPF 等内部路由协议和客户互联，BGP 本身就是一种边界网关协议，主要在自治系统之间传递路由信息，它具有丰富的属性信息、易于扩展、同时具备良好的路由控制能力，被广泛采用在大中型客户和 ISP 网络的互联路由保护中。而且由于 ISP 呼叫中心路由在骨干网中采用的是 MPLS-VPN 技术，所以我们最终决定采用 EBGp 接入 ISP 网络，具体实施过程如下。

1. 由 ISP 分配给客户两段互联地址以及内部地址段，同时分配一个私有 BGP 自治域编号 Y（假设 ISP 城域网自治域编号为 X）作为 EBGp 实现 MPLS-VPN 互联的基础。

2. 客户端路由器分别和 ISP 实现链路互通调试后，ISP 分别在两个路由器上增加 VPN 的地址家族，以思科配置简要说明步骤：

```
router bgp X
address-family ipv4 vrf vpn1111 // 假设为 vpn1 111
redistribute connected // 发布该 vpn 下的直连路由
neighbor a.b.c.d remote-as Y // 指定客户邻居
neighbor a.b.c.d activate // 激活邻居
```

// 为了网络安全配置适当的前缀列表限制进入和出去的 IP 段

```
neighbor a.b.c.d prefix-list xxx in
neighbor a.b.c.d prefix-list yyy out
```

```
no synchronization // 关闭同步
network a.b.0.0 // BGP 宣告地址段
exit-address-family
```

3. 客户端配置两台出口路由器按正常 BGP 标准配置，不再详细列出。

至此通过 EBGp 实现了动态路由的保护，解决了设备软件故障、升级、链路单通等静态路由中存在的问题，同时通过 EBGp 的前缀列表可以限制客户路由器接收的路由条目数量，降低了硬件内存、CPU 的要求。最终从软硬件多方面满足了网络接入的高稳定性需求。

内部网络保护设计

接入 ISP 网络稳定性固然重要，但是也不能忽略内部网络的路由和交换安全，否则同样会造成整体网络中断、大面积瘫痪等不可接受的故障。所以针对同时接入较多坐席或服务器的网络，同样需要实现设备和链路的保护，只不过采取的技术和广域网有所不同。

中心采用两台三层交换机（以下简称 DSW）互为备份，全部业务的三层 IP 网关均配置在 DSW 上。往上与出口路由器之间通过 OSPF 实现路由互通和保护，在本地 R1 和 R2 上配置 OSPF 和 BGP 的路由相互重分发，从而实现内部网络和 ISP 之间的全程互通。往下汇聚全部接入层交换机（以下简称 ASW），每台 ASW 分别通过内部链路连接至两台 DSW，起到链路保护的作用，同时保证在任何一台 DSW 出现故障时，不会导致下联 ASW 全部中断。

ASW 由于接入话务台数量较少，一旦硬件故障影响面不大考虑成本因素无需进行硬件双备份，如有其它业务设备接入需求可以按重要性采用直接接入两台 DSW 或者接入两台 ASW 进行保护，无需改动网络架构。

通过以上实施实现了三层路由互通和重要节点设备的保护，那么接入层的具体保护如何实现呢？大家知道网络最下层主机需要设置默认网关才能与其它网段通信，如上所述我们的网关都在 DSW 上。那么如果默认网关出现问题，出口通信还是会造成中断。要实现网关保护可以在两台 DSW 上冗余配置两个网关 IP，但是这样问题又来了，主机通常只能配置一个默认网关 IP 地址，如果配置的网关所在 DSW 设备故障，依然会导致断网（除非人工重新配置新的网关）。要解决这个问题需要采用 HSRP（Hot Standby Router Protocol）热备份路由器协议或 VRRP（Virtual Router Redundancy Protocol）虚

拟路由器冗余协议,考虑 HSRP 是思科的私有协议,所以我们选用了国际标准的 VRRP 来实现。

VRRP 的保护过程在本项目中是这样的:将两台 DSW 组成一个备份组,它们会形成一个虚拟的网关 IP,将所有主机的默认网关配置为该 IP,通过优先级配置将其中一台作为主,主路由器会主动响应主机的 MAC 地址请求,主机发往虚拟网关的数据全部由主路由器转发。通过命令配置可以实现当主路由器检测到下联链路中断后降低优先级,备路由器升为主并主动跟新 MAC 后主机流量全部由它转发,还有一种是主路由器故障宕机,备路由器检测到后升为主接管全部流量,这样就同时实现了链路和设备故障导致的网关保护切换,而在此过程中主机毫无察觉。当然为了实现 VRRP 协议的运行和主备心跳检测,两台 DSW 需要有互联链路作为心跳线存在,如果没有设计该链路,那么主备检测的心跳数据包将只能通过下联的 ASW 互通实现,这时如果有一方向链路中断可能导致双主路由器的出现,此时外网回来的

流量会部分丢失。所以为了确保心跳线的稳定,我们采用了两条互联链路的聚合捆绑。

VRRP 本身只提供了网关的保护,为了实现上行流量的负载均衡和设备的充分利用,可以将 ASW 划分成多个 VLAN 组,再根据 VLAN 组在两台 DSW 内部配置多个 VRRP 备份组,不同备份组缺省选择其中一台 DSW 作为主路由器,这样就达到了上行流量分别转发至不同的 DSW 的目标。

结语

通过方案的不断优化,实现了本中心由外到内的全程保护。由于网络技术的不断发展更新,针对二层三层、骨干、汇聚、接入、不同厂家等都有不同的保护技术和协议出现,不能逐一介绍,需要读者在实践中综合考虑成本、性能、现有设备协议兼容性、新技术等因素来设计选择最佳的保护方案。

◆ 多点视频会议连接方式比较

西安 兰珂

简单的把视频会议系统可以分为:软件视频会议系统和硬件视频会议系统。软件视频会议是基于 PC 架构的视频通信方式,主要依靠 CPU 处理视、音频编解码工作,其最大的特点是廉价,且开放性好,软件集成方便。硬件视频会议是基于嵌入式架构的视频通信方式,依靠 DSP+ 嵌入式软件实现视音频处理、网络通信和各项会议功能。其最大的特点是性能高、可靠性好,大部分中高端视讯应用中都采用了硬件视频方式。

在中大型企业中,硬件视频会议系统在会议室对会议室这种相对比较正式,参与人数较多的会议中应用十分普遍。参会的会议室的被一台视频会议设备覆盖,其中多点的视频会议系统必须由 MCU(视频会议系统中心控制设备)管理控制,整个视频会议系统就是两个或多个视频会议设备之间的互通,那么这多点的视频会议设备应该如何连接在一起?

首先先说视频会议设备,它一般包括:摄像头,主机,声音采集器这几部分组成,以宝利通 HDX8000-720P 为例,它具有高分辨率的摄像头,分辨率最低为 720P 最高可达 1080P,输出视频会议的视频、音频的多媒体流就要求最低的网络传输速率为 2Mb/s。

再说多点视频会议的网络连接。以某单位为例,所在本城市拥有两个办公地点 A 区和 B 区,北京还有集团公司总部, A 区办公有自己的办公网络出口, B 区也有自己的办公网络出口。现实的需求就是 A 区和 B 区相距 20 多公里,为了节省成本,方便办公, A 区和 B 区之间建立视频会议系统,可是两个不同的出口网络怎么连接在一起?

虚拟网络连接就是使用已经很成熟的 VPN 技术将不同区域的网络出口建立虚拟隧道进行打通实现,实现多地的网络互访互联。

使用专线互联就是租用电信运营商的线路实现多点互联,过去几年以2M的ASDL专线(电信称为DDN专线)进行连接的很多,现在随着企业级的语音通话、及时通话、视频会议及其它应用不断发展,2M的专线已经不能满足一些企业的多点连接的需要,电信运营商又推出了另一种专线光纤来满足这些企业的需求,它的速率可以达到155M甚至更高。

在我们建立视频会议系统的时候选择哪种网络连接方式就要进行一下验证,其实两种连接方式都各自有优缺点(如图1)。

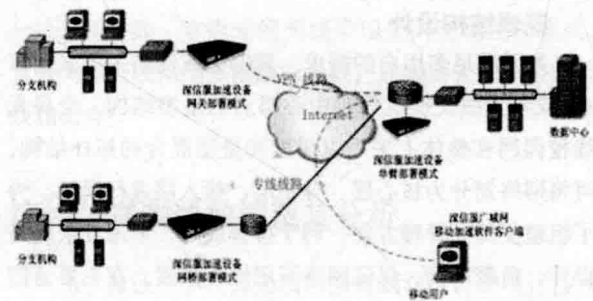


图1对比示意图

先说使用专线互联的方式,其优点就是稳定能保证网络速率,保证视频会议传输的多媒体流可以有一个稳定的传输速率,这种方式最大的缺点就是产生的持续费用高,根据电信运营商提供的大体报价:2M普通专线月成本为3600元/月/条,10M普通专线月成本为11000元/月/条,2M普通专线月成本为3600元/月/条,

10M光纤专线月成本为30000元/月/条。但是在我们单位视频会议使用的频率却是平均每周至多有一次视频会议,也就是说平时视频会议的专线就空空在浪费着。

再来说说使用虚拟VPN技术进行连接,以我们单位为例,目前两个办公区A区和B区都有深信服的IPSec VPN设备,而且已经实现了两地的VPN互联,但是目前只应用在OA办公平台的互访上,而且随着企业信息化的建设多个应用在两个办公区之间的推广,仅仅的办公上的文件数据流已经在VPN设备上显得传输有些吃力,又使用VPN进行了A区和B区的视频会议联通测试,测试发现仅仅能做到两个视频会议设备的互联,视频传输十分困难。

查阅相关资料,也咨询了深信服厂家的技术人员,制约VPN传输速率及其稳定性的因素很多,不单单有本身VPN设备的问题,还有各自两个园区出口带宽的多少,以及视频会议当中各个园区出口带宽对VPN设备是否有剩余,剩余多少的问题。

其中深信服公司新推出的广域网加速VPN设备,对其也有了解,其工作原理就是以网关或单臂模式部署在企业的网络中,在总部和各分支之间建立VPN通道,低成本代替专线实现安全可靠的互联。同时,通过多层次优化手段和专业的加速技术,提高总部和分支之间的互访速度。但是受控于此类型设备造价很高大约在150000元,且我们单位A区、B区网络出口本身很紧张等条件只好作罢此实验测试,但是在其连接速率和未来的成本节约方面以后很定会采用到。

校园无线平台构建研究

云南 徐翔俊

随着校园网络信息化普及,师生们日趋要求尽可能方便、快速、灵活的使用网络。无线校园网络平台可以实现现在教室、礼堂、会议室、图书馆、体育场馆等场所能够方便迅速的访问校园网络,让网络渗透到校园每个角落;重要的是可以实现快捷便利的办公自动化和信息化,加强学校内部各部门的业务联系,提高工作效率,

实现资源共享。

随着无线局域网技术及其产品的日趋成熟,无线网络已经广泛应用诸多领域。目前我国仅有15.1%的学校有无线校园网,但绝大多数都属于试运行阶段,并没有广泛开放;有36.2%的学校计划建设无线校园网。因此全国各校在无线网络建设上具有较大的发展空间。本文

以曲靖市某中学为例构建校园无线网络平台,阐述设计与规划校园无线局域网的原则、方法和步骤,构建基于 WLAN 的校园无线网络,同时并对相关的设计方法进行探讨,最后利用仿真软件对设计进行了模拟仿真,验证设计的合理性,为相关的研究和探讨提供参考。

中学校园无线网络规划与设计原则

校园无线网平台主要目的是为了让学校完成全方位立体式无线网络覆盖,使教职工可以依托无线网络完成各项教学及办公事务;广大师生可以利用无线网络访问校内和校外网络资源;同时需要综合考虑学校信息化需求,最大程度利用原有校园网络,节省网络投资,降低今后网络维护成本。在设计与规划中学校园无线网络时应该遵循以下原则:

- (1) 采用层次化结构,利于网络构建和维护;
- (2) 整体上采用以树型和星型混合的拓扑结构,将网络划分为核心层、分布层、接入层进行设计;
- (3) 校园骨干网采用有线方式,接入网采用无线覆盖;
- (4) 局部无线网络构建中的无线接入点(AP)的数量根据应用需求灵活布置,AP 接到各层接入交换机上,各层接入交换机再汇聚到每栋楼的汇聚层交换机上;
- (5) 无线网络以单个 AP 小面积覆盖,多个 AP 整合交叉覆盖形成大面。

案例背景及需求分析

案例中学是曲靖市的一所重点中学。该校共有教学楼(包含办公室)两幢,综合楼一幢,实验楼一幢,学生宿舍四幢。其中学生宿舍未进行网络搭建,教学楼,综合楼,实验楼分别采用有线方式建设了校园专网,没有无线网络。学校文件传输等工作必须在办公室等固定的地点进行,局限性较大,灵活性差。

该中学新构建的校园无线网络平台要求在网络互联、安全防御等方面与有线网络进行良好的兼容和互补,对无线网络进行管理和统一认证,同时做到尽可能的简化网络结构,提高网络访问速度与效率。具体需求为:在网络功能方面能满足校区之间、楼宇之间的通信,支持教学资源传输(视频、文字、图像)、提供资源共享(学习资料等)与综合服务(学校论坛,教学计划,成绩查询等);在性能方面要求校园内部的室外场所(走廊、

大厅等)速率高,安全要求一般,主要是满足在网络使用人数激增时仍然能够保证服务质量,办公室或会议室速率要求一般、安全要求高,多媒体教室或计算机机房速率要求高,安全要求低,有效地支持教学活动;在经济方面要求运营费用低,易于管理维护。

曲靖市某中学校园无线网络设计

基于中学校园无线网络规划与设计原则,以及对案例的调查和分析,本文探讨对该中学进行校园无线网平台进行规划及设计。

逻辑结构设计

为了满足多用户的需求,局部无线网络主要采用以 AP 或者无线交换机等为中心结点的星型结构。全局无线校园网在整体上采用以树型和星型混合的拓扑结构,可将网络划分为核心层、分布层、接入层进行设计。为了组建便捷、管理方便、利于排查故障,考虑冗余链路设计,负载均衡,保证网络可用性等因素,在主要通信节点上采用树型拓扑结构。

物理结构设计

该校校园骨干网通过光纤接入高速 Internet,并通过有线介质连接到配有各种网络服务器的计算机中心,然后通过无线介质将综合楼子网、教学楼子网、实验楼子网、宿舍子网等连接起来,并为室外的移动用户提供连接。其局部无线网络构建如下:

(1) 教学子网。在教学过程中,大多传送的是文本、图像和部分视频等数据,要求较高传输率,因此采用有线接入与无线接入相结合的方式。无线网络以单个 AP 小面积覆盖,多个 AP 整合交叉覆盖形成大面,覆盖区域每个 AP 都独立接到接入交换机上,以保证有效带宽。根据人数大教室可设置 2~4 个 AP,小教室可设置 1~2 个,每层的 AP 接到各层接入交换机上,各层接入交换机再汇聚到每栋楼的汇聚层交换机上。

(2) 实验楼子网。构建无线网络实验室将提供充分的网络连接灵活性,并可解决随着新设备的不断增加而改造实验室、频繁调整网络信息点的问题。对数据流量要求高的实验室可多配置 AP,对要求低的实验室可少配置 AP,每层的 AP 接到各层接入交换机上。

(3) 办公子网。办公子网主要面向学校的各级领导以及各职能部门,办公计算机所实现的功能主要是对网络数据的查询、修改、添加、删除等操作。采用高灵敏度、穿透能力强的无线 AP 产品,配合分离式吸顶天线。以

一个 AP 配合一个天线或多个天线，采用楼道安装 AP 覆盖方式以完成室内区域的完全覆盖，每层楼的 AP 数量与楼的形状有关。

无线设备的选用

无线网卡：采用 USB 接口无线网卡应用于台式机，便携式计算机采用自身的无线网卡。

无线接入点（AP）：主要技术为 802.11 系列。考虑辐射干扰因素，在校园中按照室内 30 米、室外 100 米（没有障碍物）覆盖范围，支持用户数量为 30 ~ 50 个点。

无线网桥：采用 5.8GHz 频段的 802.11a 无线网桥及其相应设备。

无线天线：室内无线天线采用全向天线工作模式，室外无线天线采用多幅扇面天线，或扇面天线和定向天线相结合。

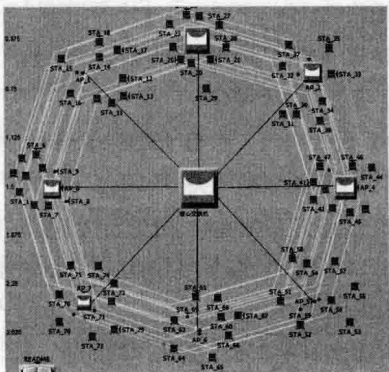
网络仿真测试数据及其分析

为了验证中学校园无线网络规划与设计的可行性及科学性，本文利用专业仿真软件 OPNET Modeler 对案例中学构建的无线校园网进行网络仿真测试。通过对仿真测试数据的分析探讨，为构建中学校园无线网络平台提供参考。

OPNET Modeler 是 OPNET 公司于 1987 年发布的第一个商业化的网络性能仿真软件，提供了具有重要意义的网络性能优化工具，可以进行预测性的网络性能管理和仿真。本文采用的为 OPNET 的 14.5 版本。

整体结构布局

根据案例中学的教室、办公室、宿舍楼的地理位置，采用星型网络为该中学的无线网络的布置。如图 1 所示为该中学核心交换机路由器的逻辑布局。



快速实现多系统集中维护

广东 黄国贤

维护现状概述

随着多网元、多设备的出现。维护员为了制作一条局数据或处理一个故障，需要在不同的设备网管终端上来回操作，有的设备更只配备一个维护台，这时工程师只能排队轮流操作，工作滞后。

目前，各电信机房普遍实行集中监控，受值班人员专业水平参差不齐的因素影响，值班人员往往一监控到告警，就直接通知相关专业人员，有时候因为值班人员的表述不清，专业人员不得不在半夜三更或在恶劣的天气里从家赶到现场，进行故障确认。

如何让维护员使用自己的电脑（不用安装专业的维护软件）对设备进行维护，而不用排队到专业网管终端上操作，如何让工程师在远程就可以对设备进行诊断，而不用盲目的赶往现场，这些非常值得探讨，该文章将从集中维护网络的搭建、维护台的配置和相关安全事项这3个方面来介绍如何实现集中维护多网元设备。

集中维护多元设备方案介绍

集中维护网的搭建

网络搭建时采用一台华为 AR-2811 路由器和一台 S3928 交换机。（随着设备的更新换代，有些交换机和路由器被淘汰下来，可以加以利用，对于交换机只要能够划分 VLAN 就行，路由器只需要支持 NAT 功能和能够支持子接口）如图 1 所示。

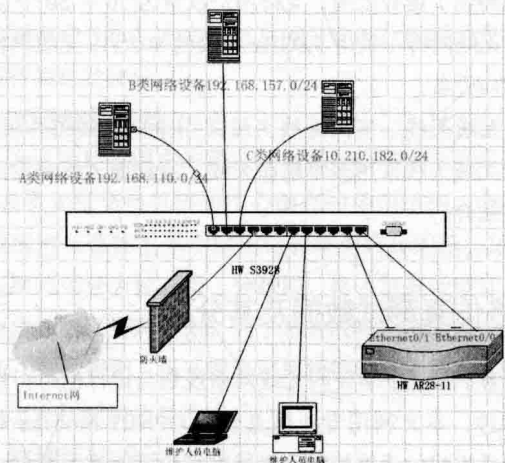


图 1 网络连接

网络连接说明：

1. 从 A 类网络设备的网络里引出一条网线接到交换机 1 口，归属于 VLAN 2。
2. 从 B 类网络设备的网络里引出一条网线接到交换机 2 口，归属于 VLAN 3。
3. 从 C 类网络设备的网络里引出一条网线接到交换机 3 口，归属于 VLAN 4。
4. 交换机 4 口连接互联网，化入 VLAN 5，该口主要用于远程 VPN 拨号进入维护网段，在远程如家里对设备进行操作。
5. 交换机 6~10 口用于维护网段，给维护人员电脑接入使用，不用划 VLAN。
6. 交换机 11 口，连接 AR28-11 路由器的 Ethernet0/1，用于维护网段的网关，不用化 VLAN。
7. 交换机 12 口启 trunk，用于连接 AR28-11 路由器的 Ethernet0/0，透传各设备网段的数据到路由器上。

交换机的配置

现在只给出 HW-S3928 各接口的配置，如下：

```
interface Ethernet1/0/1
description A communications equipment
port access vlan 2
```

```

interface Ethernet1/0/2
description B communications equipment
port access vlan 3
interface Ethernet1/0/3
description C communications equipment
port access vlan 4
interface Ethernet1/0/4
description Internet to Vpn
port access vlan 5
interface Ethernet1/0/5
interface Ethernet1/0/6
interface Ethernet1/0/7
interface Ethernet1/0/8
interface Ethernet1/0/9
interface Ethernet1/0/10
interface Ethernet1/0/11
interface Ethernet1/0/12
port link-type trunk
port trunk permit vlan 1 to 5
配置 AR28-11 路由器

```

(1)、配置 Ethernet0/1

```

interface Ethernet0/1
ip address 192.168.1.1 255.255.255.0 ----- 这里配置用于维护网段的网关

```

(2)、配置 Ethernet0/0

从 A, B, C, 互联网各取出一个地址用于 Nat 转换

```

nat address-group 1 192.168.110.33 192.168.110.33
nat address-group 2 192.168.157.223 192.168.157.223
nat address-group 3 10.210.182.211 10.210.182.211
在 Ethernet0/0 上启用子接口功能, 用于终结 VLAN
interface Ethernet0/0.1
description A communications equipment
ip address 192.168.11.0.33 255.255.255.0 ---A 类网段的接口地址

```

```

nat outbound 3001 address-group 1 -- 允许 3001 访问列表的地址访问 A 段网络

```

```

vlan-type dot1q vid 2 - 用于终结 VLAN 2
acl number 3001 - 创建标号为 3001 的访问列表

```

```

description A communications equipment
rule 0 permit ip source 192.168.1.0 0.0.0.255
destination 192.168.110.0 0.0.0.255

```

(0.0.0.255 这反掩码来决定哪些地址可以访问 A 类设备网络)

```
rule 10 deny ip
```

同理依次创建 B、C 类设备的 NAT 和访问列表。

通过以上的配置, 在维护网段就可以用一根网线同时访问 A, B, C 设备网段, 而不用频繁更换网线和网卡的 IP 地址了。

以上配置满足了本地访问需求, 若要进行远程拨号维护, 就要进行 L2TP VPN 的配置, 配置如下:

```

l2tp enable -- 启用 L2TP VPN
domain sys
ip pool 1 192.168.0.2 192.168.0.10 -- 远程拨号进来使用的地址池
interface Virtual-Template1 -- 建立一个虚拟接口
ppp authentication-mode chap domain sys
ip address 192.168.0.1 255.255.255.0
remote address pool 1 -- 远程拨号使用的地址池

```

```

l2tp-group 1
undo tunnel authentication-mandatory-lcp
allow l2tp virtual-template 1
local-user temp password simple temp@#$$% service-type ppp ----- 拨号的用户名和密码

```

以上配置完成后 L2TP VPN 服务器就已经架设好了。不过对于使用 L2tp Vpn, 客户端的 Windows 操作系统还需要进行如下配置。

(1) 修改注册表, 禁用自动 L2TP/IPSec 策略:

HKEY_LOCAL_MACHINE\System\CurrentControlSet\Services\Rasman\Parameters, 单击 Parameters 参数, 接着在右边窗口空白处单击鼠标右键, 选择 [新建 / 双字节值] 并新建一个注册表值 (名称为 ProhibitIPSec, 值为 1), 然后重新启动系统。

(2) 在网络连接里创建一个新的 VPN 拨号连接, 相关参数设置需要和路由器的配置一样。设置好后, 进行 VPN 拨号, 拨号成功后将获得 192.168.0.X 的地址, 你只要在路由器中把该地址加入到相应的 ACL number 访问列表中即可。这样你就可以在远程对设备进行操作。

维护台的设置

网络通了, 只是成功了 50%。由于电信设备的专业

维护台主要采用 Solaris 和 Windows 两种操作系统,如果要远程维护就必须把相应的电信设备配备的维护软件装入维护员的电脑,有的维护软件需要运行在 Unix 系统,有的维护软件比较大,而且要装如 Oracle, MyAQL server 等大型数据库软件,这对于电脑配置不高的维护人员来说又是一个问题。如何让维护人员的电脑不用安装消耗资源庞大的维护软件,又能轻松在不同电信设备间进行切换操作呢?

使用 Unix 系统的设备

如使用的 MOTOR 的 OMC 系统,维护员对 MOTOR 的 GSM 基站、BSC 维护,都是通过 OMC-R 维护台进行,而该维护台采用的是 Solaris 系统。直接在办公电脑上装维护软件不可能。(办公电脑大都是 Windows 系统),目前可以采用以下方案进行:

(1) 可以采用 Netterm、CRT 等终端仿真软件登入维护台进行,但是这些软件只能远程 telnet 进行命令交互。即只支持文字,不支持图形界面。

(2) 对于需要开启 GUI 图形界面界面时,Netterm, CRT 等仿真软件无法实现。以下重点介绍可以开启图形界面的 Xmanager 软件。因为网络互通是经过路由器 NAT 来进行的,所以在软件配置时需要设置代理。如图 2 所示。

设置好后直接连接,就可以象在 OMCR 维护台上一样操作了。

使用 Windows 的维护台

如使用的华为交换机维护工作站,可以利用 Windows XP 操作系统允许多用户同时登入的特点,用远程桌面连接。这样不占用专业维护台,又可以利用 Windows 自带的远程桌面连接登入专业维护台,共享该维护台对通信设备进行操作,省了在自家电脑装维护软件的麻烦。以下简要介绍 2 种配置 Windows XP 或 Windows 2000 Server 多用户功能的方法。

(1) 直接安装 WinConnect Server XP 多用户远程桌面服务器软件,这个方法简单,但是软件需要购买,不实际。

(2) 对专业维护台的 Windows XP 系统进行改造(也满足运行维护规范要求,不得在专业维护网管终端安装无关的软件),首先从网上下载 Build 2055 补丁里 termsrv.dll,在安全模式下覆盖现有系统的里的 termsrv.dll 这个文件(因为只有 Build 2055 补丁里 termsrv.dll 才可以支持多用户同时登入)。

然后修改注册表 HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Control\Terminal Server\Licensing Core 里增加 EnableConcurrentSessions="dword:00000001 这项。

最后在计算机管理里增加一个 Remote Desktop User,并允许该用户远程桌面连接。这样你的 Windows XP 多用户系统就设置好了。开启 Windows XP 自带的远程桌面连接软件进行连接(对于 Windows 2000 的维护电脑只要把 Windows XP 里的 Mstsc.exe 和 Mstscax.dll 这两个文件考过来就可以直接使用),这样就可以直接共享专业网管终端对电信设备进行操作。

安全注意事项

(1) 可以在路由器上进行 IP 地址和 MAC 地址绑定,防止部分维护员改变 IP 地址,访问未受权的设备。

(2) 设置远程 VPN 的账号与 IP 地址绑定,专人专用。在路由器上配置相应的安全策略,只开放远程拨号所需的端口。不用远程维护功能时拔掉互联网网线,需要时才叫机房人员把网线接上(机房人员需要做好使用登记),这样保证内网与互联网的物理隔离。

(3) 定期对路由器的 log 和个专业维护台的日志进行分析,查看是否有可疑的非法登入。

结语

通过集中操作维护,不仅解决了维护人员排队使用网管终端的问题,而且解决了维护人员在自己的电脑上装一大堆维护软件的麻烦。以此同时又可以远程对设备进行操作维护,对故障的抢修赢得时间。此种方案对于维护人员和需要远程办公的人员带来了极大的便利。



巧用交换机的局域网业务

福建 李贵华 陈瑜明 石海潜

VLAN 简述

VLAN(Virtual Local Area Network)又称虚拟局域网,它是一种通过将局域网内的设备逻辑地而不是物理地划分成一个个网段,从而实现虚拟工作组的技术。一个 VLAN 内部的广播和单播流量都不会转发到其他 VLAN 中,从而有助于控制流量、减少设备投资、简化网络管理、提高网络的安全性。所谓的 VLAN 技术,其实就是一个对 TAG 字段进行操作的过程。通常计算机发送或接收的数据帧是不带 TAG 字段(如果有 TAG 字段,计算机就会丢包),但数据帧进入交换机内部后,交换机会为数据帧增加一个 TAG 头,再根据 TAG 头中 VLAN ID 信息,按照规则对相应的数据帧进行处理。所有的交换机接口都有一个 PVID (Port VLAN Identity),交换机端口会根据它的 PVID,决定数据帧进入或离开时数据帧头部的 TAG 字段的处理方式。

交换机接口类型

对于日常使用的二、三层交换机,其端口接口类型可以分为三种:Access 接口、Trunk 接口和 Hybrid 接口,在这里笔者对三种端口类型作一简要介绍。Access 接口只能承载一个 VLAN 的流量,通常用于交换机与 PC 相连的接口,当 Access 接口收到一个数据帧时,先判断是否有 VLAN 信息,如果没有则打上自己的 PVID,如果有则直接丢弃;当 Access 接口要转发一个数据帧时,先判断该数据帧的 VLAN 是否和自己在一个 VLAN,如果是,则先剥离 VLAN 信息再转发,如果不是,则丢弃;Trunk 接口上可以承载多个 VLAN 的流量,一般用于交换机之间的链接。当 Trunk 接口收到一个数据帧时,先判断是否允许该 VLAN 的流量通过,如果允许则转发到相应的接口,由相应的接口进行处理;如果不允许则丢弃。Trunk 接口发送数据帧时,同样判断是否允许该 VLAN 通过,如果允许则转发到相应的接口,由相

应的接口进行处理;如果不允许则直接丢弃;Hybrid 类型的端口可以属于多个 VLAN,接收和发送多个 VLAN 的报文,可以用于交换机之间的连接,也可以用于连接用户的计算机。它是一种混杂模式,同时具有了 Access 接口和 Trunk 接口的特点,实现了在一个 Untagged 端口允许报文以 Tagged 形式送出交换机。利用 Hybrid 属性,定义分属于不同的 VLAN 端口之间的互访,这是 Access 接口和 Trunk 接口所不能实现的。Hybrid 接口和 Trunk 接口的最大区别是对任何 VLAN 打标记或不打标记。

Hybrid 接口转发数据帧的原理

当 Hybrid 接口接收数据帧时,先判断该数据帧是否有 VLAN 信息,如果有则看该接口是否对该 VLAN 打标记,如果对该 VLAN 打标记,则直接转发到相应的接口,由相应的接口进行处理;如果没有对该 VLAN 打标记,则丢弃(因为默认情况下,Hybrid 接口只允许默认 VLAN 的数据帧通过)。如果收到的数据帧没有任何标记,则标记为自己的 PVID。在接口上配置对某些 VLAN 标记所起的作用,只是允许和不允许该 VLAN 的数据帧通过,且只在接口发送数据帧时起作用。Hybrid 接口发送数据帧时,若该数据帧有标记,则判断该数据帧的标记 VLAN 和自己是否在同一个 VLAN,如果是在同一个 VLAN,则去掉标记后转发;如果该数据帧和自己不在同一个 VLAN,则判断接口对该数据帧是标记还是不标记,如果是不标记,则去掉标记后再进行转发,如果是标记则直接转发,若没有明确说明则直接丢弃。如果要发送的数据帧没有标记则直接转发。

应用 Hybrid 特性区分局域网业务实例

以笔者单位局域网的典型业务区分为例,应用二层

交换机就能实现不同 VLAN 之间同网段 PC 互访。如果利用路由器和三层交换机做访问控制列表来实现业务区分,就要麻烦得多。单位一般的业务区分为 A 区、B 区、C 区和 D 区,其 VLAN 划分分别为: vlan10, vlan20, vlan30 和 vlan40。由于网络安防和实际工作的需要, A 区主机可以访问 B 区、C 区和 D 区主机; B 区主机可以访问 A 区主机,但不能访问 C 区和 D 区主机; C 区主机可以访问 A 区和 D 区主机,但不能访问 B 区主机; D 区主机可以访问 A 区和 C 区主机,但不能访问 B。其网络拓扑图如图 1 所示。

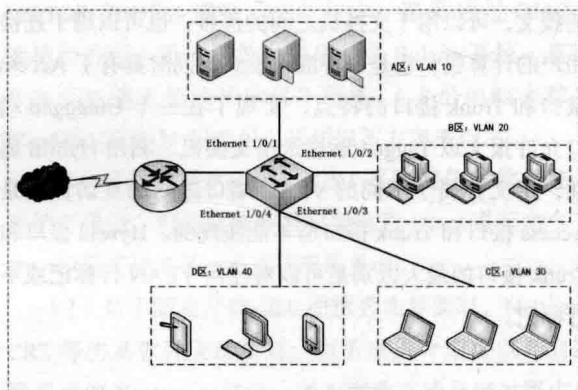


图 1 局域网络拓扑结构

以 H3C 3100 交换机为例加以说明,配置是通过 Hybrid 接口的 PVID 来表示一个端口,接收端口通过是否将 VLAN 设置为 Untagged VLAN,来控制是否与 PVID VLAN 和该 VLAN 的端口互通。

// 创建业务需要的 VLAN,并将端口 1 划分到 VLAN1 中;

```
[H3C]vlan 10
```

```
[H3C-vlan10]port ether net 1/0/1
```

// 将端口 ethernet 1/0/1 配置为 Hybrid 类型;

```
[H3C]interface ethernet 1/0/1
```

```
[H3C-ethernet1/0/1]po rt link-type hybrid
```

// 设置端口的 PVID 等于该端口所属的 VLAN;

```
[H3C-ethernet1/0/1]po rt hybrid pvid vlan 10
```

// 将互通端口的 PVID VLAN 设置为 Untagged VLAN,接收数据帧时去掉 VLAN10、VLAN20、

VLAN30 和 VLAN40 的标识符,意思就是 B 区、C 区和 D 区主机可以访问 A 区主机;

```
[H3C-ethernet1/0/1]po rt hybrid vlan 10 20 30 40 untagged
```

其余 3 个端口 VLAN、端口类型配置和上述配置基本相同,不同之处就是配置 untagged 时的允许的 VLAN 有所不同。

端口 2 具体配置如下:

```
[H3C-ethernet1/0/2]po rt hybrid pvid vlan 20
```

// 将互通端口的 PVID VLAN 设置为 Untagged VLAN,接收数据帧时去掉 VLAN10、VLAN20 的标识符,意思就是 A 区主机可以访问 B 区主机;

```
[H3C-ethernet1/0/2]port hybrid vlan 10 20 untagged
```

端口 3 具体配置如下:

```
[H3C-ethernet1/0/3]po rt hybrid pvid vlan 30
```

// 将互通端口的 PVID VLAN 设置为 Untagged VLAN,接收数据帧时去掉 VLAN10、VLAN20 的标识符,意思就是 A 区、D 区主机可以访问 C 区主机;

```
[H3C-ethernet1/0/3]port hybrid vlan 10 30 40 untagged
```

端口 4 具体配置如下:

```
[H3C-ethernet1/0/4]port hybrid pvid vlan 40
```

// 将互通端口的 PVID VLAN 设置为 Untagged VLAN,接收数据帧时去掉 VLAN10、VLAN20 的标识符,意思就是 A 区、C 区主机可以访问 D 区主机;

```
[H3C-ethernet1/0/4]port hybrid vlan 10 30 40 untagged
```

结语

在小型局域网中,利用应用交换机的 Hybrid 接口特性即一个端口可以属于多个不同的 VLAN,来完成分属不同 VLAN 内的同网段 PC 的访问需求,和使用三层交换机的访问控制列表来控制 VLAN 之间的互访比较起来,利用交换机 Hybrid 混合端口方法用起来更为方便,也可以节约购买三层交换机的成本,降低了网络的复杂度和维护难度,大家可以在平时的组网过程中试一试。

多网段监控网络聚合方法

江苏 张华 杨小泉

目前监控已经成为企事业单位、店铺、公共场所的必备设施，但许多场合的现状是每一期工程来一个施工方，每次的配置都大相径庭或自成体系，给安防部门带来工作上诸多的不便，许多企业或物业的监控室多多少少的放了几套监控设施，公共区域来一套，重点区域来一套，是不是有办法能整合在一起呢？

PC 多网卡法

这一招对多个系统或多个地址段的状况比较实用，如果一个系统内存在模拟系统、数字系统可以简单预约整合。

案例一：某企业有 5 年前安装的海康威视模拟摄像头 8 个，本次又添加了 16 个数字高清摄像头，让保安老是看两个系统似乎很不愿意，老板又坚持原有系统可以用，强烈要求保留。于是在保安室添加了一台简易 PC 机，4G 内存加 60G 固态硬盘（目前白菜价），性能非常好，配备一个 32 的液晶电视机作为显示器。网卡一设置为“192.168.18.155”接入企业内网，必要时可实现办公需求，原有模拟录像机也在此网段，可直接访问。网卡二设置为“192.168.255.199”，负责新添加数字录像机的连通。无线网卡设置为“192.168.1.199”，这样顺便可以把隔壁宿舍区的网络连接过来。一台 PC，三块网卡把三个网络整合到一起。三个网络又相互隔离，避免其他员工超权限访问或窃取资料，保证了各区域的安全性。接下来就是路由编写，编写四条路由指令，就万事大吉了。如果三个系统使用的是同一品牌的监控设备就可以用 PC 客户端实现资源的统一管理了。

本方法虽然功能比较强大，但面临如果 PC 中毒或安防人员误操作可能波及三个网络的安全；还有如果网卡更换等操作需要重新编写路由指令，需要有一定水平技术人员才能实现。

录像机多址设定

目前好多 NVR 都配置了双网口，这无疑是一个非常实用的配置，可以选择为“网络容错”和“多址设定”两种模式。首先我来做个名词解释，网络容错：就是说就是在一个局域网内为了保证网络的正常运行而做的二方面准备。优点就是当以个内网中当一条线路出问题的时候网络还能正常运行。即两个网口一个坏了，另外一个可以马上用。多址设定：即可以设置多个 IP 地址。

当我们遇到需要一套设备在内网和外网同时需要访问，且要求两个网段隔离的情况下可以采用这个方法，或者在案例一中所遇到的问题，可以用一台 NVR 同时录制两个区域的视频，同时可以向两个不同区域进行转发。如果结合 DDNS 系统，可以实现内网录像机的网络远程浏览功能，较适合小型企业、商店等环境使用。

路由器多 WAN 口法

普通我们家庭使用的路由器充其量只能所起了 NAT 转换和有线向无线转发的功能，目前的中高端路由器，除了可以实现上网功能外，这里和大家介绍一个多 WAN 口的路由器使用方法。

案例二：某机关单位，内网原有多个复杂系统，且公网路由出口走向不明，原有建设人员已经无法找到，机房交换机找不到密码无法登陆，现由于机构改革合并了另一家单位的带有监控系统 and 控制系统，甲方要求将两个系统合并到一个网络系统，且必须保留原有全部功能。

现场勘查结构是：原单位采用 10.10.10.X 网段的地址，IP 地址为指定；新合并单位采用的是 192.168.1.X 的网段地址，IP 地址为自动获得。有多台电脑需要同时使用两个网络内的资源，如果用双网口方案实现，就是要每个电脑多拉一根网线，有点难度。再三权衡后，决定采用一台企业级百兆双 WAN 口路由器来解决问题，WAN 口一为系统默认端口，IP 地址设定为网内某台计算机的地址 10.10.10.8，掩码 255.255.255.0，网关

10.10.10.1, WAN 口二指向新单位, 地址: 192.168.1.201, 掩码 255.255.255.0, 网关: 192.168.1.1。在路由器做好简单路由指向后, 此时可以将所有需要连接到两个网络的计算机通过这台路由器进行连接上网。

此案例最大的障碍就是原有网络的封闭, 无法做任何改动与查询链路信息, 通过多 WAN 口路由器的连接, 实现多 LAN 的互联。

三层交换机网关汇聚

大家知道, 广播包是大型局域网的一大杀手, 尤其是在大型监控网络中, 每个摄像头默认在发出一次 I 帧的时候就会同时发出一个广播包, 当一个网络拥有上千个终端的时候, NVR 或存储服务器端口也会不堪重负去处理广播包, VLAN 技术是一个简单可行的隔离广

播包的好方法, 这里和我大家介绍一个大型企业的监控网络的规划方案。采用了一台华为 S 5700 的交换机进行 VLAN 划分和数据交换。

其中 VLAN1000 用于交换机与上一级企业网络的互联, VLAN1406-1410 用于规划五个厂区摄像机地址, VLAN1411 用于存储服务器的地址, VLAN1462 用于布置管理平台服务器和客户端。这样的配置可以避免各个网络间相互干扰, 所有的数据交换都通过 VLAN 的接口网关地址进行转发。这样的规划可以部署超大型的监控网络或其它局域网, 且技术简单易行。

以上是我在实际工作中遇到的几个监控网络互联互通的案例, 希望能对大家在网络维护与规划的时候有所帮助。

网络考试 Kiosk 模式的探究

陕西 罗昊江 张欣

网络考试现状

网络考试系统由于依托的是网络服务器, 便于统一管理、随时组织实施, 使得我们组织实施考试更为简单、快捷。实现网络考试的方式一般有三种途径, 在下表做了比较。自主开发, 购买系统, 云服务。

基于云服务提供考试系统大多是免费使用的或者是费用低, 能大大降低学校和培训机构应用计算机网络组织考试的使用成本, 但针对这种方式其组织管理考试时需要解决防止考生作弊的问题。

问题的提出

在机房组织网络考试时, 应试者在进行网络考试的同时也可以通过 internet 访问查找考试资料、获取考试答案。而通过设置网络访问限制到相应网址的访问需要使用 3 层设备, 一方面增加了设备的成本, 另外由于是利用普通计算机房组织考试, 考试时需要限制访问, 平时上课时又得要放开限制, 会使得机房的网络管理变得复杂。采用适当的技术手段来保障网络考试中考生只能

在卷面上进行答题操作, 而无法使用除此之外的网络资源和本地资源, 就能够保证考生无法通过计算机作弊了。其实就是计算机 Kiosk 模式的应用体现。Kiosk 模式是指信息亭模式, 原意是指自助式的信息服务模式。这种模式广泛使用在商业中, 用于公共电脑或者嵌入系统, 比如 ATM 机、自动服务机之类的系统, 系统仅提供一个浏览器, 用户也仅能使用浏览器所提供的功能, 应用于网络考试中可以防止考生作弊。

由于互联网上的考试系统使用 Web 浏览器作为客户端, 使用浏览器的 Kiosk 模式就可以最大程度地减少本机的程序应用限制, 因为我们只需让浏览器能正常工作就可以了。Web 浏览器的 Kiosk 模式是一种以全屏方式显示网页的模式。不同于 F11 键切换出的全屏显示方式, 无地址输入栏, 也无菜单栏、工具栏和状态栏, 仅会显示网页与滚动条, 鼠标仅能点选网页内容, 其他操作必须依靠快捷键实现, 这些特点符合我们进行网络考试时的基本要求。

问题的解决

Web 浏览器的 Kiosk 模式比较

主流的 Web 浏览器是支持 Kiosk 模式的。通过测试发现 Kiosk 模式下 IE 支持 Kiosk 模式启动,但在点击网页链接后的新建窗口不再是 Kiosk 模式;而 Firefox 则是由第三方插件 R-Kiosk 来实现 Kiosk 模式的,它同时还能屏蔽了常用功能键和鼠标右键;比较发现 Chrome 支持 Kiosk 模式启动,点击页面链接后新建窗口覆盖原窗口并保持 Kiosk 工作模式。所以我们认为使用 Chrome 浏览器作为考试用浏览器较为合适。在浏览器工作在 Kiosk 模式下时,由于已经屏蔽了地址输入栏、菜单栏

和工具栏,结合禁用功能快捷键,考生通过 Web 浏览器访问非考试网站的问题就可以得到解决。接下来只要保证考生只能使用 Web 浏览器就可以禁止其访问本地资源。

机房在通常使用中不用限制计算机的任何功能,当其作为网络考试的场所时,可以通过这一方法实现暂时的功能限制来保障考试的管理需要。此方法简单、高效,既没有专用系统的开发成本,又充分利用了互联网考试系统的资源,适合于组织大部分课程的日常测试和常规考试。本程序及方法在我校已实际使用,达到了所需的目标效果。

◆ 浅析策略路由的使用

山东 何钰 崔冬梅

应用策略路由;必须要指定策略路由使用的路由图,并且要创建路由图。一个路由图由很多条策略组成,每个策略都定义了1个或多个的匹配规则 and 对应操作。一个接口应用策略路由后,将对该接口接收到的所有包进行检查,不符合路由图任何策略的数据包将按照通常的路由转发进行处理,符合路由图中某个策略的数据包就按照该策略中定义的操作进行处理。

在互联网快速发展的时代,各大运营商都在为提高用户上网体验做着大量的工作,为的是能够在互联网业务上占据一席之地,除了提高用户上网带宽外,还需要部署设备来满足用户观看视频和下载热门资料的要求,只有网速快了、稳定了才能真正把互联网业务发展好,把用户吸引住。最近为了有效提升用户观看视频和下载资料的体验,同时最大程度缓解互联网出口的压力,我们计划部署缓存服务器来着重解决这一问题,该服务器会根据用户访问资源的相似度,即如果多个用户都访问该资源,则视频服务会将该资源下载下来,如果再有其他用户访问此类资源,则这部分用户就会将该资源从缓存服务器上直接下载,不再从互联网上获取。因为缓存服务器部署在网络内部,用户访问的资源只要缓存服务器上有,就相当于在内网中获取,所以用户访问和下载

资源的速度上会得到明显的提升,而且用户访问的这部分资源不再占用互联网出口的带宽,这样就会大大节省了互联网出口的费用。接下来我们就部署缓存服务器的过程中使用策略路由的方法做一下介绍,首先我们先了解下缓存服务器在网络中部署的位置以及现有网络拓扑结构如图1所示。



图1 网络拓扑图

通过图1我们可以看到在网络中多台BRAS连接核心路由器1和2,其中在T8000-1上有两个互联网出口,然后使用策略路由将数据转发至不同的互联网出口,从

图 1 中我们可以看到缓存服务器部署在城区 BRAS-1 上，我们要实现的需求是 PPPoE 拨号的用户能够正常访问缓存服务器，而且缓存服务器也能正常访问 PPPoE 拨号的用户，这样既能满足用户从缓存服务器上下载资源，又能满足缓存服务器给有需求的用户发送重定向报文，这样一来一去才能完成数据的交互。既然知悉了需求，下一步就要对网络设备进行配置。从图 1 中我们可以看到 BRAS-1 连接核心路由器，我们定义缓存服务器的地址 10.220.255.10/30，首先我们解决的是从 PPPoE 拨号用户到缓存服务器的通讯，数据会先匹配策略路由转发至省公司核心路由器，这样就会造成从 BRAS-2 上发往缓存服务器的数据包出现以下路径如下所示：

```
C:\Users>tracert -d 10.220.255.10
```

通过最多 30 个跃点跟踪到 10.220.255.10 的路由

```
1<1 毫秒<1 毫秒<1 毫秒 10.220.255.17
```

```
2<1 毫秒<1 毫秒<1 毫秒 10.253.139.5
```

```
3 5 ms 10 ms 5 ms 172.16.0.89
```

```
4 5 ms 5 ms 5 ms 172.16.0.90
```

```
5 5 ms 5 ms 5 ms 10.253.139.2
```

```
6 5 ms 5 ms 5 ms 10.220.255.10
```

从上面我们可以看到在 PC 上 tracert 缓存服务器的路径是有问题的，首先 PC 发出的报文先到达网关，再到达济宁核心路由器，然后到达省公司路由器 172.16.0.89。最后才访问到服务器，这样的路径是不能满足缓存服务器工作要求的，如果拨号用户从服务器上下载资源都要从济宁互联省公司的出口上转发的话，无疑增大了出口带宽，这样就失去了我们部署缓存服务器的意义，那么如何实现拨号用户到缓存服务器是正常路径。所谓的正常路径即用户访问缓存服务器在 BRAS 之间进行转发，不再使用省公司的出口。这就涉及本文的核心部分策略路由，想必大家对路由比较熟悉，那么策略路由就是一种比基于目标网络进行路由更加灵活的数据包路由转发机制。路由器将通过路由图决定如何对需要路由的数据包进行处理，路由图决定了一个数据包的下一跳转发路由器。我们既然知道了策略路由是一种比较灵活的路由，他可以指定源地址和目的地址，以及路由转发的方向，那么我们就设想能不能实现从 BRAS 上过来的地址在匹配当前策略路由之前先转发到缓存服务器呢，经过我们对策略路由的了解，这个想法是可行的，这就需要配置策略路由，配置步骤如下所示：

```
ipv4-access-list SHENGGONGSI-1
```

```
// 定义一个名称为 SHENGGONGSI-1 的 ACL
```

```
rule 10 permit ip any 10.220.255.10 0.0.0.0
```

// 定义条目 10，任何源地址访问目的地址 10.220.255.10 动作是允许

```
route-map SHENGGONGSI permit 5
```

```
// 进入名称为 SHENGGONGSI 的 route-map
```

```
match ip address SH ENGGONGSI-1
```

```
// 匹配 SHENGGONGSI-1 ACL 中的地址
```

```
set ip next-hop 10.253.139.2
```

```
// 下一跳指向 10.253.139.2 即济宁城区 BRAS1
```

上面我们完成了 BRAS 上策略路由的配置，其中我们新建了一个名称为 SHENGGONGSI-1 的 ACL，在这个 ACL 中我们定义了什么源地址要访问缓存服务器的这么一个条目，然后在“SHENGGONGSI”的 route-map 中调用这个 ACL，动作是允许，如果匹配 SHENGGONGSI-1 的 ACL，即有访问缓存服务器的报文，就将数据下一跳转发至 BRAS-1 即缓存服务器的连接的设备。上面是我们在原有的策略路由的基础上增了一个 ACL 和 route-map，为了更好的更直观的策略路由的使用，我们下面将把策略路由列举出来方便我们查看：

```
ipv4-access-list SHENGGONGSI
```

```
rule 10 permit 10.21 9.0.0 0.0.255.255
```

```
rule 20 permit 10.22 0.0.0 0.0.255.255
```

```
ipv4-access-list SH ENGGONGSI-1
```

```
rule 10 permit ip any 10.220.255.10 0.0.0.0
```

```
route-map SHENGGONGSI permit 5
```

```
match ip address SHENGGONGSI-1
```

```
set ip next-hop 10.253.139.2
```

```
$route-map SHENGGONGSI permit 10
```

```
match ip address SHENGGONGSI
```

```
set ip next-hop 172.1 6.0.89
```

```
ip policy interface xg ei-0/0/0/1 route-map SHENGGONGSI
```

```
ip policy interface smartgroup13 route-map SHENGGONGSI
```

```
ip policy interface smartgroup11 route-map SHENGGONGSI
```

```
ip policy interface smartgroup20 route-map SHENGGONGSI
```

上面向大家展示的是一个完整的策略路由的配置，我们从上到下介绍一下，首先定义了两个不同名称的 ACL，动作都是允许不同的网段，然后最主要的是接下

来的 route-map 调用 ACL 的时候，我们注意到在两个 route-map 后面都有一个 permit 数字，这个数字代表匹配的优先级，也就是说在数据转发的过程中，首先匹配 permit5 的中的这条 ACL “SHENGGONGSI-1” 如果匹配上那么将执行转发至 BRAS-1，如果匹配不上则转发至省公司互联网出口，有了这个 route-map 匹配的先后顺序，就很容易解决我们拨号用户访问服务器的问题，总体来说如果数据报文目的地址是缓存服务器则优先转发给 BRAS-1，如果目的地址不是缓存服务器则正常转发至省公司。完成上面操作步骤后，我们在拨号上网的主机上跟踪了一下路径如下所示：

```
C:\Users\zhaozong>tracert -d 10.220.255.10
通过最多 30 个跃点跟踪到 10.220.255.10 的路由
 1<1 毫秒<1 毫秒<1 毫秒 10.220.255.17
 2<1 毫秒<1 毫秒<1 毫秒 10.253.139.5
 3 5 ms 5 ms 5 ms 10.253.139.2
 4 5 ms 5 ms 5 ms 10.220.255.10
```

通过上面我们对路径的跟踪看到拨号上网用户访问缓存服务器首先到达网关，其次是 T8000-1，然后是 BRAS-1，最后到达缓存服务器，设备配置到这里，似乎完成了配置，但是我们只是完成拨号用户到缓存服务器的通讯，如果从缓存服务器到拨号上网用户通讯的话，是不是正常数据转发呢？那么我们对路径跟踪后发现缓存服务器到拨号上网用户到达 T8000-1 后会优先匹配策略路由将数据送至省公司，这样又会占用互联网出口带宽，这样怎么办呢？仔细思考下，缓存服务器访问拨号上网的主机会将数据包转发至省公司，是因为在 T8000-1 上有策略路由的缘故，数据包按照策略路由转发，是因为数据包匹配了策略路由中的 ACL，那么我们

如果让数据包匹配不上 ACL 呢？那岂不是就不按照策略路由转发了。问题分析道这里我们立即将缓存服务器的地址段修改为 172.28.0.2，同时将 T8000-1 上的策略路由也做了调整，配置步骤如下：

```
ipv4-access-list SHENGGONGSI-1
rule 10 permit ip any 172.28.0.2 0.0.0.0
```

我们通过修改 ACL 中的目的地址来完成从缓存服务器至拨号上网用户的通讯，这样缓存服务器发往拨号上网用户的流量就匹配不上策略路由，而按正常的路由转发，反过来从拨号上网的用户访问缓存服务器，首先匹配这条 ACL “SHENGGONGSI-1”，如果匹配上就把数据发送至缓存服务器，如果不是访问缓存服务器的数据包则直接转发至省公司。这样数据在一来一回的过程中都是正常转发的，这样就算是满足了服务器部署的基本要求，至于缓存服务器的配置这里就不再叙述。

刚才我们通过定义 ACL，然后在 route-map 中调用 ACL，最终在互联 T8000-1 的端口上调用策略路由实现拨号上网用户可以按照正常路径访问服务器。后期我们又修改了服务器的地址，将 ACL 中的目的地址也做了相应的调整，这样就满足了缓存服务器至拨号上网的用户使用正常路径的转发。这次在网内部署服务器，对于初次接触大型电信级路由器的我们来说，在配置路由的时候特别担心会中断网络，其实这种担心是有必要的，毕竟是单位的核心设备，这也从侧面反映了我们对设备配置的不熟悉，后期我们将认真学习配置手册，然后利用新开业务的机会进行设备的配置，以期尽快达到熟悉配置路由器的目的，这也是我们将来工作学习的而一个主要方向。

❖ ACL 在网络中的应用

▼ 山东 韩磊

公司某部门办公场所迁移时提出了一个新需求：该部门要自己组成一个小范围内的局域网，内部资源共享，对外进行隔离，即使同样 C 类网段同样 VLAN 下的其

他部门电脑，也不能访问。

由于各种布线，VLAN 设置等历史原因，决定采用 ACL 访问控制列表的方式，将该部门独立出虚拟的局域

网络，并与其外部进行隔离。

公司内网段设置为 10.66.66.0，其中网关设置为 10.66.66.1。此部门的机器 IP 比较分散。其他部门的 IP 也分散穿插在其中。部门搬迁后从网关交换机的 47 口出去，引到其办公室，然后经过办公室内的几台交换机到每个坐席的位置上。

网关交换机是华三的，经过查询文档，以及跟华三工程师的交流，最终通过配置交换机的 ACL 访问控制列表，隔离出一个虚拟的小局域网。

华三交换机的 ACL 配置命令

通过 telnet 连接到该交换机。

先进入超级管理员模式，键入 su，然后键入密码。

进入配制模式，键入 sys。

配置一个允许访问列表，为的是允许局域网里的机器访问外面的网络。需要配合端口控制命令使用。

```
acl number 3000
```

```
rule permit ip source any destination 10.66.66.1 0// 允许任何 IP 访问 IP 10.6 6.66.1, 0 代表是具体设备的 IP 地址。
```

```
rule permit ip source any destination 9.0.0.0 0.255.255.255 允许任何 IP 访问 A 类地址段 9.0.0.0, 0.255.255.255// 是该地址的反码。
```

配置一个允许被访问的列表，为的是允许局域网内的机器可以接受到外网的数据信息。这个要配合端口控制命令使用。

```
acl number 3001
```

```
rule permit ip soucre 10.66.66.1 0 destination any// 允许 IP 10.66.66.1 访问所有 IP。
```

```
rule permit ip source 9.0.0.0 0.255.255.255 dest ination any// 允许 A 类地址段 9.0.0.0, 反码 0.255.255.255 访问所有目标 IP
```

配合上面的两个 ACL 表进行使用。

```
acl number 3002
```

```
rule permit ip source any desitnation any
```

定义，添加相关 ACL 表使用的逻辑，其中 hjzx, hjzx_out, hjzx_deny 为定义的类型。

```
traffic classifier hjzx operator and
```

```
if-match acl 3000
```

```
traffic classifier hjzx_out operator and
```

```
if-match acl 3001
```

```
traffic classifier hjzx_deny operator and
```

```
if-match acl 3002
```

```
traffic behavior hjzx_deny
```

```
filter deny
```

```
traffic behavior hjzx
```

```
filter permit
```

定义策略

```
qos policy hjzx_out
```

```
classifier hjzx_out behavior hjzx
```

```
classifier hjzx_deny behavior hjzx_deny
```

```
qos policy hjzx
```

```
classifier hjzx behavior hjzx
```

```
classifier hjzx_deny behavior hjzx_deny
```

应用到端口上

进入对应端口 47

```
interface gigabitethernet 1/0/47
```

47 口下局域网设备访问该端口的策略应用

```
qos apply policy hjzx inbonud
```

47 口将数据传输到其下局域网的策略应用

```
qos apply policy hjzx_out outbound
```

保存配置

输入 quit 退出配置模式。输入 write file，命令行提示是否保存，选择 y 即可。

至此局域网与正式隔离完毕。



网络打印新经验

威海 赵永华

在 Windows 中快速安装共享打印机

当我们需要将网络打印机添加或安装到 Windows 时,往往习惯通过系统提供的添加打印机向导工具完成,其实有一种更快速的方式,这里以英文版 Windows 8 为例,实现过程为:打开“Computer or Network”,浏览到“Network”后找到共享计算机及打印机后右击打印机后选择 Connect。

将网络打印机添加为 Windows 系统本地打印机

有一次,笔者在添加共享打印机时出现问题,后来改变思路,将其添加为本地打印机时得以成功。笔者于是总结出—条经验就是,有时解决问题的方法就是回避问题。具体而言,此时需要知道分配给该打印机的 UNC 名称或者 IP 地址,这并不难,打印机本身的状态页面就显示出有关详情。在英文版 Windows 8 中具体操作过程为:从开始菜单打开“Devices and Printers”窗口,点击顶端工具栏中的“Add a Printer”后选择“Add a local printer”;然后选“Create a new port”,在端口类型中选“Local Port”后点击“下一步”。

在 Port Name 栏目需要输入 UNC “\\192.168.1.100\hpprinter”,之后设置就不多说了。

为笔记本设置“对位”打印

笔者本本的默认打印机是“随位应变”的,在家里是家里的普通打印机,到了办公室则变为另一台商用型打印机,那么这种自动识别不同打印机的“智能化”是如何实现的呢?在英文版 Windows 8 中是这样的:从开始菜单打开“Devices and Printers”窗口,选择好有关打印机后点击窗口顶端用于管理默认打印机的工具栏“Manage default printers”,然后选择“Change my default

printer when I change networks”(意即当网络改变后改变默认的打印机);接下去,对每个网络,从“Select network”列表中选择对应的网络名,并同时从“Select printer”列表中指定默认的打印机,设置妥当后点击按钮“Update”或者“Add”即可。

通过第三方软件管理网络打印

有些 IP 管理软件如 Free IP Switcher 及 NetSetMan 在网络打印方面其实大有用武之地。这里,笔者推荐惠普开发的 WebJetAdmin。WebJetAdmin 能自动搜索网络上的打印机,能识别和管理惠普全系列网络打印机,对第三方网络打印设备也能实现发现、状态显示等功能,能清楚显示连接在网络上的网络打印机数量、设备型号以及 IP 地址等。透过设备状态窗口,能直观地看到粉盒中墨粉的剩余量,打印机是否正在打印作业,纸张是否用完,甚至还能看见当前打印机控制面板的消息和图标,用于远程地将打印机脱机或将其联机,避免了管理员奔波于各打印设备间低效工作的局面。网打管理软件的控制面板和帮助功能,能协助用户确定打印机故障,使整个打印过程更轻松、便捷。

WebJetAdmin 还提供了创建队列、警报、网卡固件的更新等等网络打印机的管理窗口。如果条件允许,可以在局域网里设置打印服务器,所有其他的客户机都可以通过该打印服务器打印(尤其是对一些硬件配置低的老机器),这样既可简化安装设置,又可以在打印服务器上监视客户机的打印队列;还可设置警报。

使用虚拟打印机

实际应用中我们在打印之前想要预览从而避免浪费纸墨,排版满意后再打印。此时可以安装一个虚拟打印机。虚拟打印机同真实打印机一样,安装完毕,打开“控制面板”中的“打印机和传真”,会看到所安装的虚拟

打印机,可以像使用一台打印机一样使用它们。鼠标双击将其打开,可以对其“打印首选项”和“属性”进行修改,从而设定是否共享、可使用时间、是否后台打印和优先级,以及纸张大小、版式安排等。它们同样能截获所有 Windows 程序的打印操作,或模拟打印效果,或完成某一特殊功能。有些软件自带虚拟打印机,有些则是专门的虚拟打印机,利用这些虚拟打印机,可以帮助我们完成很多特殊的任务。

这里介绍 Windows 8 如何连接安装虚拟打印机:(1)在 Windows 8 桌面按 Windows+X 键,打开系统菜单,从弹出菜单中选择“控制面板”命令;(2)在“控制面板”中点击“查看设备和打印机”,点击工具按钮栏的“添加打印机”按钮;(3)在打开的“添加打印机”中点击“我需要的打印机不在列表中”,选择最下面的“通过手动...”单选项,再点击“下一步”; (4) 选择“创建新端口”,并选“Local Port”,再点“下一步”; (5) 在“端口名”对话框中输入端口名,点击“确定”按钮; (6) 从左边选“Microsoft”,在右边的“打印机”中选择你所需要的虚拟打印机,再点“下一步”; (7) 给新添加的虚拟打印机设置一个名称,设置好后点“下一步”按钮; (8) 提示成功后,我们可点击“打印测试页”按钮看看是否

添加成功,返回“设备和打印机”窗口中可以看到成功添加的虚拟打印机。

手机和平板电脑也能“网打”

目前市面上具备 Wifi 无线连接功能的打印机数量越来越多,例如佳能 MG5280 喷墨一体机和三星 ML-1865W 激光打印机。其内置 WiFi 模块,拥有一键设置功能,连接无线网络更容易,只需选择接入点(路由器)上的 WPS 按键,再按动打印机上的 WPS 按钮即可轻松完成。手机与它的连接非常简单,不需要安装任何驱动程序,更不需要连接电脑。手机和平板电脑要实现网络打印并不困难。具体设置如下。

首先需要在手机或平板电脑上安装应用程序。无论是 Android 系统,还是 iOS 系统都可以在应用市场找到具体应用程序如“Samsung Mobile print”,在网络较佳时下载安装耗时不用 1 分钟;安装完成后桌面会增加一个新的图标,点击即可进入,不需要进行任何系统设置的修改,应用程序如 Samsung Mobile print 能自动检测到三星 WIFI 无线打印机,并锁定目标,除了可以直接打印网页外,还可以打印照片、PDF 文档。

网络设备数据采集与分析

湖北 杜致远

本文作者经过研究发现通过 SecureCRT 软件与日志数据提取软件结合,成功地实现数据实时采集,并将获取数据导入 Excel 中进行统计分析。本次研究对象为无线控制器内实时用户数量。产品为锐捷 M8610-WS。

打开 secureCRT 软件并登录无线控制器,启用会话日志记录,执行如下脚本。

```
for (i=1;i>0;i++) { // 循环
    crt.Screen.send ("show clock"+"r\n"); // 显示时钟
    crt.sleep (500); // 暂停 0.5 秒
```

```
crt.Screen.send (" show WLAN-co su"+"r\n"); // 显示无线汇总
```

```
crt.sleep (180000); // 暂停 3 分钟
}
```

不关闭 CRT 程序让其自动运行一天或若干天后,已成功采集数据到日志文件中。

在日志文件由于存在许多无效信息,数据无法直接导入数据到分析系统中,如图 1 所示。最后在网上搜索到一款 refine 日志数据提取工具的软件,如图 2 所示,根据每行提取字符行特征,成功提取时间、10、20、

30、40 等五行中数据并成功生成对应 5 个文本文件。

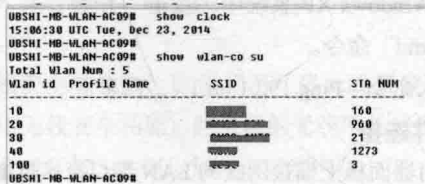


图 1 分析系统

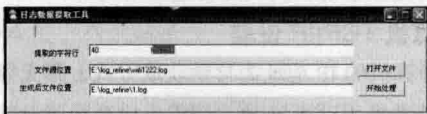


图 2 日志数据提取工具软件

将得到 5 个文件导入电子表格 (Excel) 后, 删除无关字段, 这样就得到无线设备每 3 分钟在线用户情况, 时间、WLAN10、WLAN20、WLAN30、WLAN40 四组数据, 这样你可以根据自己需要进行数据分析了。由于本校中 WLAN10、20、30 属于一家运营商, 并将此三项数据累加, 以时间、WLAN (10、20、30)、WLAN40 为数据源得到如下折线图, 如图 3 所示。

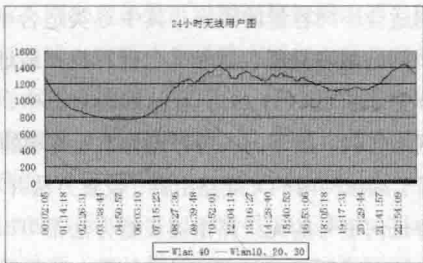


图 3 折线图

CRT 程序每个版本程序执行脚本命令格式略有不同, 此脚本文件命令在 CRT6.5 版本上测试正常。如有不能执行情况, 请在你使用版本下执行创建脚本命令, 然后将需要执行命令执行一篇, 对生成脚本进行修改编辑使其可以根据自己要求执行即可。

本文命令等待时间为设置为 3 分钟, 是为保证 telnet 操作不因超时而退出, 如果你需要更长等待时间, 就配置 telnet 超时时间为更长时间。

如果在 CRT 脚本运行期间, 出现网络设备故障, 就会造成 CRT 命令执行中断而退出, 则需要重新登录。

执行脚本前, 一定要校对网络设备时间, 避免因时间影响实际结果。

局域网无线路由设置方法

北京 刘洪波

在技术飞速发展的今天, 智能手机、平板电脑、笔记本等无线设备已经广泛流行, 目前网络可以分为有线网络和无线网络, 二者根本的区别再于, 有线网络是通过网卡、网线与交换机相联接, 无线网络是通过无线网卡与无线交换机相联接; 而且各自有各自的特点, 有线网线通过网线与交换机联接, 优点是传输速度快, 抗干扰能力强, 缺点是联接麻烦, 而且要事先布线; 无线网络是通过无线与交换机联接, 优点是安装方便, 不需要事先布线, 缺点是传输速度慢, 抗干扰能力差; 正是由于无线网络安装方便这种特点, 无线网络得到了前所未有的迅速普及。无线网络较之有线网络具有布线简单, 安装方便, 使用便捷, 美观大方等优点。

在各个单位内部, 所有职工们都希望没有网线的束

缚, 自由方便的选择不同终端畅游互联网。

“工欲善其事, 必先利其器”, 想要拥有便捷的无线网络, 必须配备无线路由器, 并且进行正确的设置。本文向您介绍的就是在局域网中无线路由器的设置方法。

无线路由器的一般设置方法

首先介绍一下 IP 地址的概念, IP 地址 (Internet Protocol Address) 翻译为互联网协议地址或者网际协议地址, IP 地址是 IP 协议提供的一种统一的地址格式, 它为互联网上的每一个网络和每一台主机分配一个逻辑地址, 以此来屏蔽物理地址的差异。Internet 委员会定义了 5 种 IP 地址类型, 即 A 类、B 类、C 类、D 类、E 类,

它们分别适合不同容量的网络，其中 C 类适合小型局域网，每个网络最多只能包含 254 台计算机，地址范围是 192.0.0.0 至 223.255.255.255，在这四段号码中，前三段号码为网络号码，剩下的一段号码为本地终端的号码。

应用于局域网内的无线路由器，设置方法并不复杂，任何品牌任何型号的无线路由器设置方法都可以概括为更改 LAN 口 IP 地址、设置静态 IP 地址和设置密码这三步。更改 LAN 口 IP 地址是确保无线路由器的 IP 地址与局域网内其他 IP 地址没有冲突；设置静态 IP 地址是使用局域网内的固定 IP 地址以获得上网权限；设置密码是控制无线网路的用户接入。

这里我以较为常用的 TP-Link 无线路由器为例介绍无线路由器的一般设置方法。

当我们拿到一个全新的路由器时，首先需要确认它之前是否被设置过，如果没有，就可以直接连接线路开始设置，否则，就要先对其进行复位操作。TP-Link 无线路由器正确的复位方法是，先将路由器接通电源，按住后面板上标识为 QSS/RESET 的按键，持续 5 秒钟以上，保持按压的同时观察 SYS 指示灯，当该指示灯由缓慢闪烁变为快速闪烁状态时，则表示路由器已成功恢复出厂设置，此时松开该按键，路由器重新启动。

硬件连接

LAN (Local area network) 是局域网的意思，LAN 接口主要用于路由器与局域网连接，WAN (Wide area network) 是广域网的意思，WAN 口主要用于路由器与广域网连接。所以，硬件连接方法是，用网线将计算机和路由器 LAN 口相连接，将路由器 WAN 口和局域网网口相连接，连接好电源，路由器将自行启动。

建立正确的网络连接

首先，查看路由器的 IP 地址，一般是 192.168.1.1，写在标签上贴在路由器背后。

然后，进行计算机 IP 地址的设置。

打开的“网络连接”界面，右键单击“本地连接”，选择“属性”，在“本地连接 属性”界面中双击“Internet 协议 (TCP/IP)”，打开“Internet 协议 (TCP/IP) 属性常规”界面，将 IP 地址设置为无线路由器的 IP 地址所在的网段，即 1 网段，所以 IP 地址为 192.168.1.x (x 的范围是 2 至 254)，子网掩码为 255.255.255.0，网关为 192.168.1.1。有时我们为了方便选择“自动获取 IP 地址”点击确定即可，如果路由器支持自动获取 IP 地址方式就没问题，否则还是需要如上所述进行手动分配 IP 地址。

当网络不通时，可以使用 Ping 命令测试与路由器是

否连通。测试方法如下：

在 Windows XP 系统中，点击“开始”—“运行”，输入“cmd”命令。

输入命令：Ping 192.168.1.1，回车。

硬件连接

路由器面板上插接网线的 LAN 端口指示灯 Link/Act 和计算机上的网卡指示灯必须都是亮的。若不亮，查看端口是否连接正确，网线是否连接松动。

计算机 TCP/IP 设置

若计算机的 IP 地址为自动获取方式，则无须进行再设置。若选择手动设置 IP，请重点检查网段设置是否与路由器在同一网段。

设置无线路由器

打开浏览器，在地址栏中输入路由器的 IP 地址：192.168.1.1，则会出现登录界面，查看路由器的用户名和密码后输入，一般用户名和密码的出厂默认值均为 admin，点击确定后进入路由器 WEB 管理界面开始设置。

更改 LAN 口的 IP 地址

在路由器界面左边菜单栏选择“网络参数”，LAN 口设置，将路由器 IP 地址设置在与局域网不同的网段，本文为方便说明，将其设置为 192.168.6.1。重启路由器。

设置静态 IP 地址

在各单位的局域网内一般是要求进行 MAC 地址绑定后才拥有上网权限的，所以应首先联系信息管理员，他会将该无线路由器 WAN 口的 MAC 地址与分配给你的静态 IP 地址绑定后将网络使用权限授权给你，将该 IP 地址设置在无线路由器的方法如下：

确认计算机使用的 IP 地址网段与无线路由器在同一网段后，打开浏览器，登录 192.168.6.1，左侧列表菜单里依次选择“网络参数”，“WAN 口设置”，选择“静态 IP 地址”，按照信息管理员分配的地址，依次输入 IP 地址、子网掩码、网关、DNS 即可，保存设置。

设置密码

在浏览器里登录 192.168.6.1，左侧列表菜单里依次选择“无线设置”，“无线安全设置”。

无线状态，作用是开启或者关闭路由器的无线功能。SSID，是服务集标识，设置任意字符串以便标识无线网络。

信道，设置路由器的无线信号频段，推荐选择“自动”模式，设置路由器的无线工作模式，推荐使用 11bgn mixed 模式。

频段带宽，设置无线数据传输时所占用的信道宽度，

可选项有 20M、40M 和自动。

最大发送速率，用来设置路由器无线网络的最大发送速率。

无线安全选项中，取消“不开启无线安全”设置。如果关闭无线安全功能，路由器的无线网络就没有加密功能，此时任何人都可以加入该无线网络。

选择“WPA-PSK/WP A2-PSK”方式进行加密，在 PSK 密码中输入密码，密码要求为 8-63 个 ASCII 码字符或 8-64 个十六进制字符，这个密码就是每一个使用该无线路由器上网的终端都需要输入的密码。有的路由器还有“认证类型”和“加密算法”选项，分别选择“自动”和“AES”即可。

如果选择“不修改无线安全设置”，则无线安全选项中将保持上次设置的参数。如果从未更改过无线安全设置，将保持出厂默认设置，即关闭无线安全。

点击下一步，保存设置，重启，设置生效，这时 TP-Link 无线路由器的基本设置就完成了。

特殊情况下无线路由器的设置方法

如上所述，设置无线路由器的基本方法是更改 LAN 口 IP 地址、设置静态 IP 地址和设置密码共三步，可有时我们会发现手里的无线路由器压根就只有有线网口，此时找到 WAN 口并设置它是关键，还是以 TPLINK 路由器为例进行说明。

更改 LAN 口 IP 地址

登录无线路由器的 WEB 管理界面，将 LAN 口 IP 地址改为 192.168.6.1。

设置路由器

登录路由器 WEB 管理界面，在“设置向导”菜单列表里选择 Router 工作模式。对于这个路由器来说，也只有 router 模式可以将有线网口设置为 WAN 口。点击下一步。

选择“WPA-PSK/WP2-PSK”，设置 PSK 密码，点击下一步。

选择静态 IP 方式，点击下一步，在出现的界面里输入信息管理员分配的 IP 地址、子网掩码、网关、DNS，保存设置后重启路由器，设置生效。

克隆 MAC 地址

完成以上两步后，将无线路由器接入局域网，仍然

不能正常上网，现象是可以搜索到该路由器，信号也满格，也可以输入密码，无线路由器却无法正常使用。用计算机以无线方式登录该路由器 WEB 管理界面，查看左侧列表菜单“网络参数”，这时与设置前不同的是，可以看到 LAN 口、WAN 口、MAC 地址克隆三个菜单项，而且，LAN 口和 WAN 口的设置都正常，点击 MAC 地址克隆菜单项，将计算机的 MAC 地址克隆到无线路由器上，测试则可以正常登录互联网。

无线路由器的安全策略

无线网络由于其简单便捷使之在很大程度上替代了有线网络，可是有一个问题摆在面前让我们有所顾虑，那就是安全问题。

根据 IEEE802.11 标准，一般无线路由器所能覆盖的最大距离通常为 300 米，实际当中真正能达到的覆盖范围主要取决于环境的开放与否，即在设备不加外接天线的情况下，视野所及之处约 300 米范围内，若是半开放性空间，或有隔离物的区域，传输约为 35-50 米左右，若借助外接天线，根据天线本身增益情况，传输距离可以达到 30 ~ 50 公里甚至更远。无线路由器覆盖范围是一个开放的空间，如何确保无线路由器的使用安全无疑是个重要问题，下面就重点介绍无线路由器的安全策略。

设置密码

目前 WEP 加密已经不太可靠，使用相关软件就可以将其破解，所以采用具备 WPA 加密的无线宽带路由器并开启 WPA 功能，手动设置密码的方法，即本文前面提到的设置密码方法。定期更换密码也可以有效防止无授权终端使用该无线路由器。

修改默认设置

众所周知，无线路由器的默认 IP 地址一般为 192.168.1.1，登录用户名和密码一般是 admin，有经验的用户只要多试几次，就可以很容易的进入无线路由器的 WEB 管理界面，了解相关信息。所以，一是我们最好将默认的 IP 地址修改为不易猜测的 IP 地址段，例如 192.168.70.1；二是修改登录用户名和密码，操作方法是使用“系统工具”菜单列表里相关功能进行修改。修改完成后，重启路由器，修改生效。

重命名并隐藏 SSID

SSID (Service Set Identifier) 的意思是服务集标识，SSID 技术是将一个无线局域网分为几个需要不同身份验证的子网络，每个子网络均需独立的身份验证，只有

通过身份验证的用户才能进入相应子网络，从而防止未被授权的用户进入本网络。

通俗讲，SSID 可以理解为由无线路由器架构起来的无线网络独有的个性化名称。需要注意的是，同一生产商推出的无线路由器都使用了相同的 SSID，无授权终端可以使用通用的初始化字符串与无线路由器建立连接，所以建议将 SSID 重新命名。

运用无线路由器的隐藏 SSID 功能，使无线路由器对其他设备不可见，再辅以 WPA 加密，降低了被搜索到的可能性。SSID 隐藏 SSID 的基本方法是在“无线设置”，“无线基本设置”，将广播（SSID）功能关闭。隐藏 SSID 后，该无线网络就不会出现在其他人搜索到的可用网络列表里，我们自己还可以正常使用网络，只是无线网络的效率会有所降低，但以此换取网络安全性的提高，笔者认为值得的。

关闭 DHCP 服务器

DHCP（Dynamic Host Configuration Protocol），即动态主机设置协议，是局域网的网络协议，使用 UDP 协议工作，主要用途有两点，一是给内部网络用户自动分配 IP 地址，二是用于内部网络管理员管理所有计算机。主机自动分配 IP 地址给每台终端，省去了手动配置 IP 地址的麻烦。如果关闭 DHCP 应用，终端用户则无法自动获取 IP 地址。停用 DHCP 的方法是不勾选“将路由器用作 DHCP 服务器”选项。

关闭无线路由的 DHCP 功能后，终端用户需要手动设置无线网卡的 IP 地址，使之与无线路由器的 IP 地址位于同一网段。例如无线路由器修改后的 IP 地址为：192.168.70.1，那么无线网卡的 IP 地址即可设置为：192.168.70.X，X 的范围可以是 2-254 之间的任意数字，默认网关与无线路由的 IP 地址保持相同。

完成以上四步基本设置，无线网络已经较为安全，但如果想让无线网络的安全防护能力有质的提升，那还可以进行下面的设置。

启用 MAC 地址过滤

保护无线网络最安全最有效的方法，也是我们强烈推荐的方法是 MAC 地址过滤。MAC 地址过滤功能就是在无线路由器中绑定 MAC 地址，在“允许”列表中一一添加已授权终端，在“禁止”列表中一一添加无授权终端，从而达到有效控制终端用户的目的。在启用 MAC 地址过滤功能时，一定要看清过滤模式是“允许”还是“禁止”，因为不同的厂商，过滤模式会有不同。

当使用允许列表模式时，是把允许终端添加到列表

中，其他不被允许的终端是无法加入该无线路由器的。

使用禁止列表也是必要的，三十六计中有一计是知己知彼百战不殆，若能够知悉不被允许的终端的相关信息，就可以有针对性的进行预防。知悉不被允许终端相关信息的途径是查看无线路由器的系统日志，通过正在通讯的计算机列表，就可以找到它，然后禁止它，即把不被允许的终端 MAC 地址加入无线路由器的设置中。

关闭无线网络

保护无线网络安全最绝对最直接的办法，应该是关闭无线网络，这样非法入侵者即使再有能力也无法进入你的网络。所谓的“关闭”其实并不是说不让大家使用无线网络，而是倡导大家养成良好的无线网络使用习惯，即，在不需要无线网络的时候，关闭无线网络功能，从而降低非法用户入侵的可能性。

具体操作方法是打开 Web 管理界面，关闭无线开关。进入 Web 管理界面进行手动开关无线网络，并等待无线路由器重启，这一操作过程确实比较麻烦，如果无线路由器具有外置无线网络开关功能是最好不过了，可以简单控制无线网络目前市场上仅有少数的无线路由器设计了外置无线网络开关，绝大多数无线路由仍需要希望未来推出的无线路由器都能加入外置无线网络开关这一功能，让用户可以更好的掌控自己的无线网络。

结语

综上所述，无线路由器的设置方法可以总结为更改 LAN 口 IP 地址、设置静态 IP 地址和设置密码这经典三步。在体验精彩无线的同时，安全也不能忽视，首先是最简单也是最基础的设置，即无线加密，推荐选择 WPA-PSK/WPA2-PSK 的 AES 算法加密；二是修改默认设置；三是重命名并隐藏 SSID；四是停用 DHCP 功能；五是启用 MAC 地址过滤；六是“WPS”一键加密功能。以上前四步，已经可以基本确保无线网络的安全。第五步是保护无线网络最安全最有效的办法。第六步安全效果也同样出色，值得大家进行深入学习。

无线路由器的设置方法并没有想象中的困难，只要好好研习，就能够轻松的驾驭它。如果想要拥有便捷安全的无线网络，就请打开你的无线路由器，和我一起进行更加深入的研究学习吧。希望本文能够抛砖引玉，可以促进广大网络爱好者学习进步，从而更好的服务于我们的工作和我们的事业。

NetAdmin World 2017

第2章 系统维护

Exchange 群集复制配置与管理

▼ 顾武雄

Microsoft Exchange Server 是现今很多企业使用的邮件服务器，而在 Exchange Server 2007 版本中，对于用户邮箱所提供的特殊故障转移功能，也是许多企业网管员的最爱。但许多人不了解它的管理方法。本文针对准备导入或测试 Exchange Server 2007 CCR 架构的企业 IT 人员，介绍如何以最简单、最快速的方式，将它部署在 Windows Server 2008 操作系统的群集故障转移 (Failover) 环境下，让即使发生了单一 Exchange Server 2007 服务器的宕机，仍然可以持续提供内外客户端的正常存取。

明白 HA 架构支持

在 Exchange Server 2007 版本以前，我们经常提到关于最新群集故障转移架构构建 (Cluster) 的方法，不过当时所介绍的部署架构是最常见的共享存储方式 (Shared Storage)。到了 Exchange Server 2007，则是改为采用节点和文件共享多数仲裁 (Node and File Share Majority Quorum) 的群集架构基础，来部署 Exchange Server 2007 SP1 的群集连续复制 (CCR, Cluster Continuous Replication)，用这种不会因为单点失败 (共享储存设备的损毁) 问题而造成 IT 服务的中断，来提供企业一个真正永不中断的服务平台。

采用 CCR 的优势

这种采用异步复写的高可用性架构有哪些优点呢？请看以下说明。

1. 不需要共享的储存设备，更不需要采用相同的服务器硬件规格。
2. 提供一个不会因服务器发生单点失败，而造成用户无法存取邮箱的解决方案。
3. 保证数据与服务 的可用性 (HA, High Availability)。
4. 针对目前的数据库，提供了最佳的数据备份中心。
5. 针对任何单点失败的灾害发生时，提供最迅速的系统与数据的恢复速度。

6. 提供企业 IT 一个最低成本与最高执行效率的高可用技术。

7. 对于许多专业的 IT 来说，这也是最简易部署的高可用性架构方法。

SP1 版本后的增强功能

从 Exchange Server 2007 SP1 版本开始 (目前最新版本为 Service Pack 3)，还可以进一步让高可用性的状况，从灾害恢复中分隔开来，并且可以在不同的状况下针对组织的需求部署自定义的组态设置。以下说明在 SP1 更新中所新增与改善现有高可用性的特色项目。

1. 备用连续复制 (SCR, Standby Continuous Replication) 功能，适用邮件邮箱在异地备份的持续备份。
 2. 支持构建在最新的 Windows Server 2008 操作系统上，这包括支持多重子网络 (multiple subnet) 的群集故障转移、支持采用动态 IP 地址 (DHCP IPv4) 的配置、对于 IPv6 地址配置的支持、新的仲裁模型 (磁盘及档案共享)。
 3. 在群集连续复制的环境中，可通过热备的群集网络进行连续复写 (记录文件传送及植入)，设置方法则是预先经由全新 Enable-Continuous ReplicationHostName 命令来设置即可。
 4. 让 IT 人员可修改群集邮箱网络名称资源的 TTL 时间，以便符合跨子网络的 CCR 高可性的故障转移规划要求。例如，可将默认 20 分钟的 TTL 设置值变更为 5 分钟 (300 秒)，只要下达 cluster.exe res <CMS NetworkNameResource> /priv HostRecordTTL=300 命令格式来变更设置即可。
 5. 报告、监控功能以及运行效率效能的改善。
 6. 邮件传输缓存区功能的改善。
 7. 提供新的 Test-ReplicationHealth 命令来诊断 CCR 的复写操作状况。
 8. Exchange 管理控制面板的操作接口改良设计。
- 最新 Exchange Server 2007 Service Pack 3 官方下载

网址：

<https://www.microsoft.com/zh-CN/download/details.aspx?id=24111>

架构准备与基础设置

构建 CCR 前的准备工作

1. 已经在相同的 Active Directory 网域中完成了集线传输服务器 (Hub Transport Server) 与客户端存取服务器 (Client Access Server) 的安装。

2. 在两部故障转移群集节点服务器上预安装好网页服务器 (IIS) 以及应用程序服务器角色相关组件, 其中在 IIS 部分还必须记得包含 IIS 6.0 相关管理工具的一并安装。

3. 在两部故障转移群集节点服务器上, 预安装好 Windows PowerShell 以及故障转移群集功能的相关组件。

4. 完成两部故障转移群集节点服务器的网络设置。

请从“服务器管理员”接口的“角色”节点页面中, 点选“新增角色”连接所预先完成的网页服务器 (IIS) 以及应用程序服务器角色的安装。紧接着, 在从“服务器管理员”接口的“功能”节点页面中, 点选“新增功能”连接预先完成的 Windows PowerShell 以及故障转移群集功能的安装。

完成了 Windows Server 2008 相关服务器角色与功能的安装之后, 接下来必须在这两部准备担任 CCR 邮箱的服务器上, 完成相关网络的安装与必要的设置。

首先在这两部服务器上确认已经完成了两块网络卡的安装, 以及设置好了公用网络 (Public Network) 与专用网络 (Private Network) 的 TCP/IP 设置, 并且建议您网络的命名上可以取名为 Public 以及 Private 即可。

请注意, 专用网络的设置, 如果您并没有打算构建跨越多重子网 (Subnet), 那么可以直接使用一条跳接的 RJ45 网线来直接对接即可。

接下来设置网络服务联机的顺序, 请在“进阶”的下拉选单中点选“进阶设置值”, 执行之后将会开启“适配卡及连接”的页面, 在此请由上而下将 Public、Private、远程存取联机依序进行排序即可。

最后, 在“Internet Protocol Version 4 (TCP/IPv4)”的属性中, 点选“进阶”按钮, 执行之后, 请切换到“WINS”页面, 并且选取“停用‘NetBIOS over TCP/IP’”设置, 点选两次“确定”按钮完成设置。

设置 Windows Server 2008 群集故障转移

在完成了前面的准备工作之后, 接下来我们便可以在 CCR 群集邮箱的其中一部主机上, 完成双节点群集故障转移服务器的设置。

首先从“系统管理工具”的下拉选单中, 点选开启“故障转移群集管理”界面, 在这个界面中目前并没有设置任何的群集服务, 请点选位于“动作”窗格中的“建立群集”连接继续。

第一次执行“建立群集”连接时, 将会开启简介说明页面, 在此说明中, 主要是建议在建立群集之前, 最好先完成“验证设置向导”的执行, 以便确认目前的硬件兼容性与硬件设置符合群集构建的基本需求。

在此笔者省略了这项验证的操作, 原因是在下一个向导设置的过程中, 一样可以完成这个验证操作。点选“下一步”。接下来在出现的“选取服务器”页面, 您可以直接输入两部 CCR 群集邮箱服务器的名称, 或是点选“浏览”按钮将它们添加到下面的清单中。点选“下一步”继续。

在接下来出现的“验证警告”页面中, 会出现群集设置验证测试的报告似乎遗失或不完整的警告信息, 这是由于我们在准备建立群集之前并没有完成验证测试所致, 不过没有关系, 请确认目前选择了默认的设置项目。点选“下一步”开始进行相关的验证操作。

此时会出现“验证设置向导”页面, 您可以看到所有相关的说明, 点选“下一步”。在“测试选项”的页面中, 您可以决定是选择“执行所有测试”还是“仅执行选取的测试”。如果选取后者, 则可以在下一步的页面属性中自定义所要测试的项目, 在此我们采用默认的“执行所有测试 (建议选项)”项目, 点选“下一步”继续。

在“确认”页面中可以看到所有即将进行验证的项目, 点选“下一步”之后将会来到“正在确认”页面, 您必须在此等待所有验证的项目都完成检查为止。验证设置向导的最后, 将会来到“摘要”的显示页面, 这里有一段信息告知我们测试已经顺利完成, 设置似乎适合进行群集。如果您想要查看更进一步的验证报告, 请点选“检测报告”, 然后点选“完成”按钮即可。在一个典型验证设置的报告中, 您可以看到所有详细的检查项是否成功。

接下来回到建立群集向导的设置页面, 完成群集名称以及群集 IP 地址的设置, 而这些信息在目前的网络中都是不能重复的。在“确认”页面中, 可以看到设置确认页面。点选“下一步”, 此刻系统便会开始根据我

们前面所设置的群集节点成员、群集名称以及群集 IP 地址来建立新的群集网络。

在“摘要”页面，您可以看到它出现了找不到仲裁磁盘的可用磁盘信息，不过这没有关系，因为我们一会儿就可以从故障转移群集的管理界面中完成这项必要的设置，需要的话，您可以点选“检测报告”按钮来查看更进一步的信息。图 1 便是初步完成双节点群集网络的范例，在笔者所建立的 EXCLUSTER.msft.com 群集页面，可以清楚地看到目前的仲裁设置所出现的信息是“节点多数 - 警告：节点失败会导致群集失败，请检查节点的状态”。



图 1 检测已完成的基础群集

群集的两个常见疑问解答

为什么需要准备 Cluster 环境？

由于 CCR 的故障转移功能是由 Microsoft Windows Cluster Services (MSCS) 所提供，因此在运行环境的部署中，操作系统必须采用 64 位的 Windows Server 2003 R2 企业版，或是本文所介绍的 Windows Server 2008 企业版，否则将会导致无法完成 CCR 的设置。

当发现准备的操作系统为标准版时怎么办？

笔者曾经在部署 Windows Server 2008 群集的环境时，正准备要开始建立群集，却发现不小心安装成 Windows Server 2008 标准版了，这时候只要将 Windows Server 2008 企业版的安装光盘拿来进行操作系统的升级即可解决。

CCR 仲裁与服务角色设置

正确设置 CCR 群集仲裁

根据以上的仲裁设置信息，告诉了我们必须变更相关的仲裁设置。请在目前的群集节点项目点击鼠标右键，点选位于“其他动作”子选单中的“设置群集仲裁”继续。接下来将会打开“设置群集仲裁向导”页面，属性中说

明了正确设置仲裁的必要性与时机。点选“下一步”继续。

在出现的“选取仲裁设置”页面中，有四种仲裁设置可以选择，分别是节点多数、节点与磁盘多数、节点和文件共享多数仲裁、没有多数只有磁盘，请在选取“节点和文件共享多数仲裁”项目之后，点选“下一步”继续。

如何快速确认群集状态

注意

想确认它目前的运行状态，只要通过两个命令参数来检测其状态即可。首先在命令提示列上输入 Cluster group，来得知目前所有的群集组是否是在联机状态。接着可以输入 Cluster node 命令参数，来得知目前所有的群集节点服务器是否是在联机与执行的状态下。

在“设置文件共享见证”页面中，您必须点选“浏览”按钮来指定一个共享文件夹存放共享见证资源所需要的文件，但是此文件夹必须具有群集系统管理员完整的访问权限，并且请勿将此文件夹建立在群集中的任何服务器上。在“确认”页面中，可以看到前面所做的设置值，确认无误后点选“下一步”来完成群集仲裁的设置。最后，在“摘要”页面中会显示完成群集仲裁设置的相关信息，若想查看进一步的相关信息，请点选“检测报告”，否则请直接点选“完成”即可。

当我们完成了群集仲裁设置之后，再一次回到故障转移群集的管理界面时，将会发现原有惊叹号的警告信息已经不见了，取而代之的是显示前面所设置好的节点和文件共享多数仲裁的设置值。

开始安装 Exchange Server 2007 CCR 服务器角色

前面我们已经完成了群集环境的准备工作，接下来便可以开始将 Exchange Server 2007 的相关 CCR 邮箱服务器构建在这上面。请在 Exchange Server 2007 SP1 的安装主选单中，点选“步骤 4：安装 Microsoft Exchange Server 2007 SP1”连接继续。您也可以使用最新版本的 Exchange Server 2007 SP3 来完成此安装设置。

接下来首先在“Exchange Server 2007 SP1 安装程序”页面点选“下一步”继续。在“安装类型”页面中，点选“自定义 Exchange Server 安装”项目之后，点选“下一步”。在“服务器角色选取”页面中，由于必须先完成主动群集邮箱角色的安装，因此请将“Active Clustered Mailbox Role”项目勾选，然后点选“下一步”。

在“群集设置”页面中，请先选取“群集连续复制”

项目，然后为这个新的群集邮箱服务器名称输入全新的命名。至于群集邮箱服务器数据库文档的路径，则可以根据实际需求来变更（因为可能后端有连接特定的 SAN 设备），但是必须注意的是，在后续的备用邮箱角色安装设置中，也必须一样才可以。点选“下一步”。

在“群集 IP 地址设置”页面中，必须至少设置一个群集 IP 地址（第一个子网络），而 IP 地址的指定方式也可以采用 DHCP 的方式来寻址。至于第二个子网络的设置部分，也只有在构建跨子网络（Subnet）的 CCR 规划中才需要设置。在“整备检查”页面中，如果是采用测试用的 32 位版本 Exchange Server 2007，便会出现相关警告信息，如果没有其他错误信息，请点选“安装”即可。一旦成功完成安装，便会出现 Exchange Server 2007 SP1 主动群集邮箱角色的显示页面。请点选“完成”按钮即可。完成安装之后，将会出现必须在重新启动之后才能够使相关的变更生效，请在点选“确定”之后重新启动服务器操作系统。

备用群集设置与最终测试

CCR 备用群集邮箱角色安装

完成了 Exchange Server 2007 SP1 备用群集邮箱角色节点的安装之后,紧接着必须到另一个节点服务器上来安装备用的群集邮箱角色,整个安装过程相当简单,只要在 Exchange Server 2007 SP1 的自定义角色安装页面中,选取“Passive Clustered Mailbox Role”项并且点选“下一步”来完成安装即可。

在 Exchange 管理控制台中如何得知邮箱服务器为群集架构

请在 Exchange 管理控制台中先点选“服务器设置”节点，然后点选位于“动作”窗格中“检测”的“新增/移除字段”，执行后您可以将默认未加入到右边窗格的字段（其中便包括了一个“群集”字段），点选“新增”按钮来加入即可。

在主要与备用的群集邮箱角色都完成安装与重启之后，请开启 Exchange 命令控制台，并且如图 2 所示输入 `Get-StorageGroupCopyStatus` 命令，来查看目前的复制状况。过程中您可能会如同范例一样先看到目前还在初始化阶段，等过几分钟之后再输入一次相同的命令，则将会看到出现正常的 `Healthy` 状态。

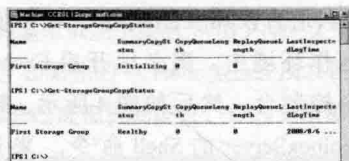


图 2 检测 CCR 群集复制状态

至于在 Exchange 管理控制台的检测部分，您可以在“服务器设置→邮箱”节点页面中，看到在范例中所建立 CMS01 的群集邮箱服务器项目，我们可以點選位于“动作”窗格中的“属性”，来查看进一步的相关信息。开启了 CMS01 群集邮箱服务器的属性之后，请切换到“群集邮箱服务器”的页面，便可以看到群集相关的详细信息，以及目前活动中的节点是以哪一部主机为主，需要的话，还可以进一步变更有关于故障转移可用性的设置值。

检测 CCR 群集邮箱服务器状态

对于群集邮箱服务器的管理，在 Exchange Server 2007 的管理控制台中，还可以直接点选位于“动作”窗格中的“管理群集邮箱服务器”，来开启“管理群集邮箱服务器”页面，以便决定是否要立即将群集邮箱服务器移动至另一个节点，还是要对于群集邮箱服务器进行启动或是停止。在群集邮箱服务器的命令控制台管理部分，首先可以如图 3 所示输入 Get-ClusteredMailboxServerStatus 命令，来检测目前群集邮箱运行的状态。

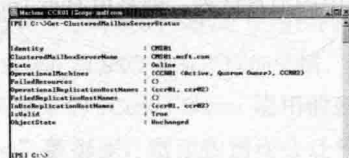


图 3 检测群集邮箱服务器状态

如果回到故障转移群集管理界面中，系统管理员便可以点选各别群集节点来进行查看，必要的时候，同样可以点选位于“动作”窗格的“其他动作”中来执行相关的管理操作，例如启动与停止群集服务等。

而在群集资源的管理中，您可以在故障转移群集管理界面中，针对目前运行的CCR群集与相对的群集资源，点选位于“动作”窗口中的动作，例如将群集资源脱机或是进行模拟此资源失败的测试操作等。

CCR 群集故障转移测试

如果想要进行这两个群集节点的转移测试，则可以针对此 CCR 群集节点 项目，按下鼠标右键，点选“将此服务或应用程序移动到另一个节点”即可。不



图 4 手动 CCR 故障转移迁移测试

Hub Transport 主机上的 Dumpster

在 CCR 架构中的事务历史记录档 (transaction log) 复制传送与 Replay 部分, 是由 Exchange Server 2007 负责处理而非 Windows Server 2008 群集服务, 至于传送过程中的消息队列, 则是由 Hub Transport 上的

Hub Transport 主机上的 Dumpster

在 CCR 架构中的事务历史记录档 (transaction log) 复制传送与 Replay 部分, 是由 Exchange Server 2007 负责处理而非 Windows Server 2008 群集服务, 至于传送过程中的消息队列, 则是由 Hub Transport 上的

[illegible]

图 5 设置 Dumpster

结语

以一个服务端的系统来说，命令管理工具的使用永远是不可缺少的，因为再设计精良的图形操作接口，也难以掌控整个系统的运作管理。对于网管员来说，必须在系统管理模式中，整理出符合自己习惯且有效率的管理方法，而在这个方法中，必须要结合图形操作接口与命令管理接口两种相辅相成的运作，才能够让 IT 维护工作达到运用自如的优化境界。

❖ 升级 vSphere 实例

▼ 河北 王春海

某小型数据中心，由 3 台 IBM 3650 M4、1 台 IBM 3700 存储组成，3 台服务器安装了 VMware ESXi 5.5，由 vCenter Server 5.5 管理。在这个数据中心部署了 VMware View 6.0 虚拟桌面、VMware vCenter Operations Manager 5.8.1。整个拓扑如图 1 所示。

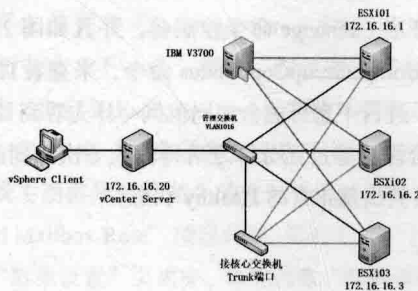


图 1 拓扑结构

升级的主要流程

1. 备份 vCenter Server。使用 VDP 备份重要的虚拟机。
2. 升级 vCenter Server 5.5 到 vCenter Server 6.0。
3. 在保证业务不中断的前提下，依次升级每台主机。

假设先升级 A，之后升级 B 和 C。在升级 A 时，将 A 置于“维护模式”，热迁移 A 上的主机到 B、C，之后升级 A。升级 A 成功（完成）后，将 A 取消维护模式。之后升级 B，最后升级 C。

下面我们将详细介绍每一步操作过程。

当前主机

在升级之前，主要做的工作是备份重要的虚拟机、修改必要的配置。

1. 备份重要的虚拟机，如果有 VDP，则提前一天使用 VDP 备份所有重要的虚拟机。对于 vCenter Server 5.5 本身来说，可以使用 vSphere Client 或 vSphere Web Client，使用自带的工具，将 vCenter Server 5.5 本身的虚拟机，克隆出一个新的副本，如图 2 所示，图中名为“vCenter_5.5(bak)-16.20”是从“vCenter-16.20”的克隆，原来 vCenter Server 安装在名为“vCenter-16.20”的虚拟机中。我们克隆一份完整的副本，是避免由于升级失败造成 vCenter Server 不能启动，而造成的影响。实际上，从 vCenter Server 5.5 升级到 6.0 是比较安全、可靠的，但为了避免出现问题，还是备份一下比较好。

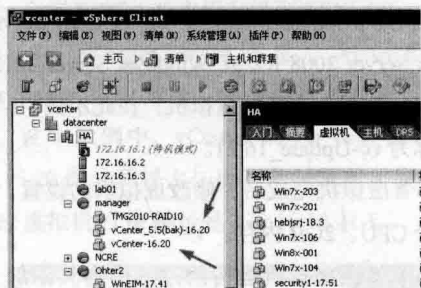


图 2 使用虚拟机“克隆”备份 vCenter Server 虚拟机

2. 如果当前是“群集”的环境，群集中有处于待机或休眠的 ESXi 主机，请打开主机电源，并修改群集配置，暂时禁用“电源管理”功能。

升级 vCenter Server 5.5 到 6.0

在升级 vCenter Server 5.5 之前，要检查你的 vCenter

Server 5.5 的虚拟机至少要有 8GB 内存、2 个处理器（如图 3 所示）。如果你的 vCenter Server 所在的虚拟机不符合要求，请修改虚拟机的配置，使其满足需求。

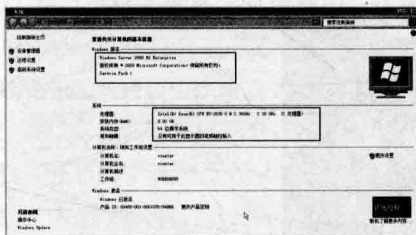


图 3 检查 vCenter Server 配置

在条件符合之后，加载 vCenter Server 6.0 的安装光盘（镜像），运行 vCenter Server 6.0 的安装程序，开始升级，步骤如下。

1. 在 vCenter Server 6.0 安装界面，选择“适合于 Windows 的 vCenter Server”，单击“安装”按钮。
2. 在“欢迎使用 VMware vCenter Server 6.0.0 安装程序”对话框，安装程序提示“此计算机上检测到 vCenter Single Sign-On 5.5 和 vCenter Server 5.5，并将升级到具有嵌入式 Platform Services Controller 的 vCenter Server 6.0.0”，单击“下一步”按钮。
3. 在“最终用户许可协议”对话框，单击“我接受许可协议条款”，单击“下一步”按钮。
4. 在“vCenter Single Sign-On 和 vCenter Serve 凭据”对话框，输入 vCenter Single Sign-On（SSO）的管理员密码，并选中“为 vCenter Server 使用相同的凭据”。如果 vCenter Server 与 SSO 具有不同的凭据，请分别输入。
5. 如果原来的 vCenter Server 使用的是“Microsoft SQL Express”数据库，则该数据库会迁移到 VMware vPostgres。

6. 在“配置端口”对话框，显示了 vCenter Server 相关服务的端口。

7. 在“目标目录”对话框，选择当前 vCenter Server 6 部署的存储位置。在此对话框显示了将原来 5.x 数据库导出的位置。

8. 在“准备升级”对话框，单击“我确认已备份此 vCenter Server 计算机和嵌入式 Microsoft SQL Server Express 数据库”，单击“升级”按钮。在此页中还提示，在将 vCenter Server 5.5 升级到 6.0 后，当前 vCenter Server 许可将处于“评估模式”。

9. 之后将开始升级 vCenter Server 5.5，并显示安装进度。

10. 经过一段时间，vCenter Server 5.5 升级到 6.0 完成，此时在“安装完成”对话框，会提示“您的 vCenter Server 5.5 已升级到版本 6.0.0”（如图 4 所示）。

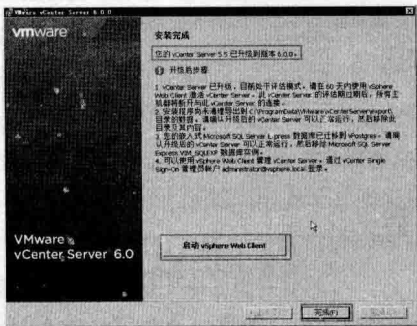


图 4 安装完成

升级 vSphere Client

在升级 vCenter Server 之后，对应的 vSphere Client 也要升级。升级 vSphere Client 很简单，你可以运行 vCenter Server 6.0 安装光盘中的 vSphere Client 安装程序，也可以使用原来的版本连接 vCenter Server，会自动提示升级。

1. 使用 vSphere Client 连接 vCenter Server (如图 5 所示)。

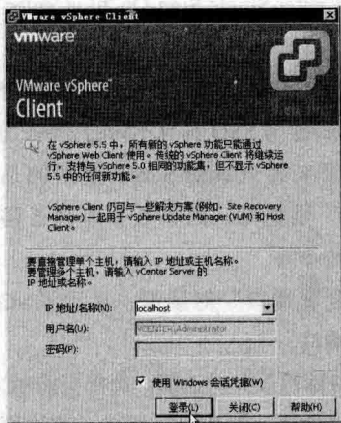


图 5 连接 vCenter Server

2. 如果当前 vSphere Client 与所连接的 vCenter Server 版本不一致，就会弹出“正在更新”的对话框，单击“运行安装程序”，会自动从 vCenter Server 下载对应的 vSphere Client 安装程序。

3. 更新下载完成之后, 单击“确定”按钮。

4. 之后进入 vSphere Client 6.0 的安装程序，选择安装语言，单击“确定”按钮。

5. 进入 vSphere Client 6.0 的安装程序。

注意 ➤

说明: vSphere Client 的不同版本可以“共存”,所以在安装高版本或低版本 vSphere Client 的时候,不会卸载原来的 vSphere Client 版本。在安装之后,在同一个 vSphere Client 中,就可以管理不同的 vCenter Server 或 ESXi。

6. 之后, 根据向导安装 vSphere Client, 直到安装完成。

7. 再次登录 vCenter Server, 会弹出“您的评估许可证将会在 X 天后过期”。

之后进入 vCenter Server 管理界面，为 vCenter Server 6 添加许可。

安装 vCenter Server Update Manager

在升级 vCenter Server 5.5 到 6.0 之后，接下来需要升级 VMware ESXi 主机到 6.0。升级的办法有两种，一种是用 vCenter Server 6 中的 Update Manager 来升级，另一种是使用 VMware ESXi 6.0 的安装镜像，通过安装镜像升级 ESXi 5.5。在本文中，我们使用前者来升级。

可以将 vCenter Server Update Manager 安装在 vCenter Server 的虚拟机中，但我们推荐为 vCenter Server Update 服务器专门创建一个虚拟机，为此虚拟机分配 2 个 CPU、2GB 内存、300GB 硬盘空间，为这个服务器规划 IP 地址为 172.16.16.21。

1. 使用 vSphere Client 登录 vCenter Server，从 Windows Server 2008 R2 或 Windows Server 2012 R2 模板虚拟机，部署一个新的虚拟机，在此示例中，该虚拟机的名称为 vc-Update 16.21。

2. 部署虚拟机完成后，修改虚拟机的设置，为其配置为 2 个 CPU、2GB 内存。

3. 如果要在虚拟机运行的过程中为其添加 CPU 及扩充内存, 在“选项→高级→内存 /CPU 热挺拔”选项, 启用内存热添加及 CPU 热添加功能 (如图 6 所示)。

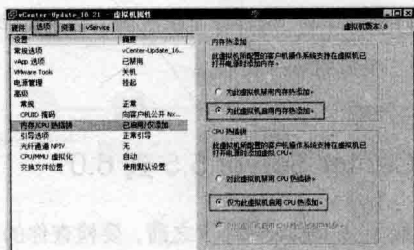


图 6 内存与 CPU 热添加

4. 之后打开该虚拟机的电源，并打开虚拟机的控制台。

注意

说明：vSphere Update Manager 需要至少 120GB 的空间，如果你的虚拟机硬盘空间比较少，可以修改虚拟机的设置，为虚拟硬盘扩充空间。在本示例中，原来虚拟机的硬盘是 60GB，我们扩充为 300GB。在进入虚拟机之后，打开“服务器管理器→存储→磁盘管理”，将空余的空间创建分区并分配盘符为 D。

5. 之后加载 vCenter Server 6.0 的安装程序，开始 Update Manager 的安装，主要步骤如下。

(1) 运行 VMware vCenter Server 安装程序，选择“vSphere Update Manager”，单击并选中“使用 Microsoft SQL Server 2012 Express 作为嵌入式数据库”，单击“安装”按钮。

(2) 进入 Update Manager 安装程序，在开始安装前可以选择安装语言。

(3) 之后开始 Update Manager 安装程序。

(4) 在安装之前，安装程序会检测当前的系统环境。安装程序要求 Microsoft .NET Framework 3.5 SP1，如果没有，开始安装之前先安装此软件。

(5) 在安装 .NET 3.5 之后，进入安装向导。

(6) 在“许可协议”对话框，接受许可协议。

(7) 在“支持信息”对话框，显示了 Update Manager 会将 ESXi 5.X 主机升级到 ESXi 6.0。

(8) 在“vCenter Server 信息”对话框，输入 vCenter Server 的 IP 地址、管理用户名及密码（如图 7 所示）。在本示例中，vCenter Server 安装在 IP 地址为 172.16.16.20 的计算机上，而当前计算机（安装 Update Manager 虚拟机的 IP 地址是 172.16.16.21）。



图 7 输入 vCenter Server 位置和凭据

(9) 在“VMware vSphere Update Manager 端口设置”，

指定指 Update Manager 的 IP 地址（安装程序自动从当前系统读取）和各个服务端口，基本在此页选择默认值即可。

(10) 在“目标文件夹”对话框中，选择 VMware Update Manager 的安装位置，以及配置修补程序下载位置，在此将补丁程序位置改为 D 盘，其他保持默认。

(11) 在“已做好安装程序的准备”对话框，单击“安装”按钮，开始安装。

(12) 之后开始安装，直到安装完成。

启用 Update Manager 插件

在安装 vSphere Update Manager 之后，需要在 vSphere Client 中加载 Update 管理客户端插件才能使用，步骤如下。

1. 使用 vSphere Client 登录 vCenter Server，在“插件”菜单中选择“管理插件”。

2. 在“插件管理器”中，在“可用插件”中的“VMware vSphere Update Manager 扩展”选项中，单击“下载并安装”链接。

3. 之后进入 vSphere Update Management Client 安装程序。

4. 进入 VMware vSphere Update Manager Client 安装向导。

5. 之后根据向导安装，直到安装完成。

安装完成后，关闭 vSphere Client，并再次进入，在“主页→解决方案和应用程序”中，可以看到“Update Manager”已经出现（如图 8 所示）。

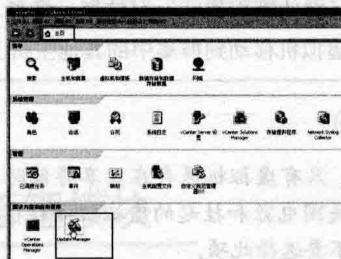


图 8 Update Manager

升级 ESXi 主机

当前网络中有三台 ESXi 主机需要升级，在升级的过程中，为了避免业务中断，在升级前，需要将要升级的主机置于“维护模式”，这样处于维护模式的主机中

的虚拟机，会迁移到其他主机继续运行。在迁移的过程中，正在运行的虚拟机不会受到影响，这样保证了业务的连续性。

1. 升级流程

在升级的时候，不是三台主机一起升级，而是一台依次升级，总体的升级流程如下（以网络中有 A、B、C 三台主机为例）：

（1）修改 vSphere HA 的设置，取消 DPM 功能。如果有处于待机状态的主机，请打开主机电源。

（2）将其中一台主机置于“维护模式”，例如 A 主机，在 A 处于维护模式前，会将 A 上正在运行的虚拟机，自动迁移到 B、C 主机。

（3）使用 Update Manager Client，导入 VMware ESXi 6.0 安装镜像，升级 A 主机。

（4）A 主机完成升级之后，将 A 主机退出维护模式。

（5）升级 B 主机，B 主机重复（2）~（4）的操作。

（6）B 主机完成升级之后，升级 C 主机，将 C 主机重复（2）~（4）的操作。

2. 升级操作

在下面的过程中，我们以升级 B 主机为例，其他主机升级与此类似。

（1）使用 vSphere Client 登录 vCenter Server，右击“群集名称”，选择“编辑设置”。

（2）在“vSphere DRS → 电源管理”中选择“关闭”，关闭 DPM 功能。

（3）如果有处于“待机模式”的主机，请右击该主机，打开该主机的电源。

（4）右击要升级的主机，选择“进入维护模式”。

（5）在“确认维护模式”对话框，选择“将关闭电源和挂起的虚拟机移动到群集中的其他主机上”。

注意

说明：只有虚拟机保存在共享存储时才选项此项，如果关闭电源和挂起的虚拟机保存在主机本地存储，则不要选择此项。

（6）等所有虚拟机都迁移到其他主机后，当前主机进入维护模式。之后在“主页”菜单选择“Update Manager”。

（7）进入 vCenter 的 Update Manager 管理界面（如图 9 所示）。

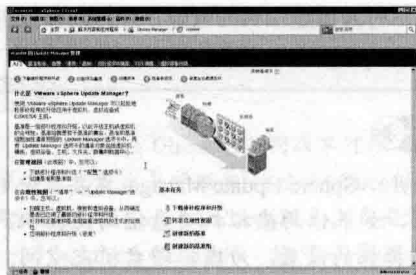


图 9 Update Manager 管理界面

3. 上传 ESXi 6.0 镜像

Update Manager 是 VMware 的补丁管理程序，不仅可以升级 ESXi，还可以为 ESXi 主机安装补丁。在本文中，只是介绍其升级 ESXi 主机的功能，首先介绍上传 ESXi 6.0 镜像的方法，主要步骤如下。

（1）在“vCenter 的 Update Manager 管理”中，在“ESXi 映像”选项卡中，单击“导入 ESXi 映像”链接。

（2）在“打开”的对话框中，选择 VMware ESXi 6.0 安装镜像。

（3）在“选择 ESXi 映像”对话框中，已经加载了 ESXi 的镜像。

（4）在“上载 ESXi 映像”对话框，显示了上载成功的 ESXi 镜像的名称、版本等信息（如图 10 所示）。

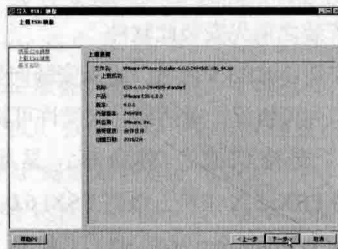


图 10 上载 ESXi 映像

（5）在“基准名称”对话框，在“名称”文本框中，为上载的 ESXi 映射设置一个名称及描述信息，在此设置名称为“ESXi 6.0.0”。

（6）上载。

4. 升级主机

将 ESXi 6.0 安装镜像上传到 Update Manager 之后，就可以升级主机了，主要步骤如下。

（1）在左侧选中要升级的主机，在“Update Manager”选项卡中，单击“附加”链接（如图 11 所示）。

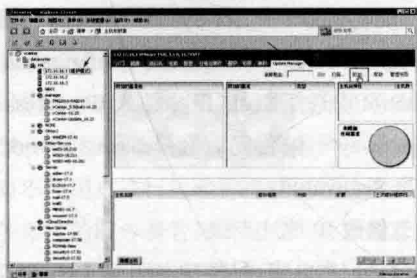


图 11 单击“附加”链接

(2) 在“附加基准或组”对话框,选择“升级基准→ESXi 6.0”,然后单击“附加”按钮。

(3) 返回到 vSphere Client,单击“修复”按钮。

(4) 在“修复选择”,选择“升级基准→ESXi 6.0.0”,单击“下一步”按钮。

(5) 在“最终用户许可协议”对话框,接受许可协议。

(6) 在“ESXi 6.0 升级”对话框,单击“下一步”按钮。

(7) 在“调度”对话框,指定修复任务的时间,选择“立即”。

(8) 在“主机修复选项”对话框,指定修复任务的维护模式选项,因为我们已经将主机置于维护模式,所以直接选择默认值即可。

(9) 在“群集修复选项”,可以根据需要选择暂时禁用的群集功能。在当前群集中主机数量较小的时候,可以选择“禁用高可用性接入控制”选项,其他选项根据需要选择。单击“生成报告”可以查看有关当前配置和更改的报告。

(10) 在“即将完成”对话框,显示了修复设置信息。

(11) 之后 Update Manager 会将升级镜像上传到要升级的主机,并自动重新启动远程主机,在升级的过程中,正在升级的主机会断开连接,这是正常现象。在“近

期任务”中可以看到升级的详细信息与提示。

(12) 等待一段时间之后,ESXi 主机升级完成。在左侧选中主机,在右侧可以看到当前 ESXi 的版本已经是 6.0.0。之后右击该主机,退出维护模式。

(13) 定位到“配置→软件→已获许可的功能”选项中,单击“编辑”链接。

(14) 在“分配许可证”对话框,为升级到 ESXi 6.0 的主机分配 vCenter Server 中添加的许可,或者通过“输入密钥”方式,输入新的许可。

(15) 之后参照上面的步骤,将第二台主机置于维护模式,并升级到 ESXi 6.0。

(16) 最后升级第三台主机到 ESXi 6.0。

等所有主机升级完成后,修改群集配置,在“电源管理”中启用 DPM 功能(如图 12 所示)。

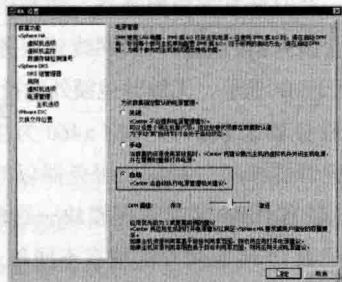


图 12 启用电源管理

至此升级完毕。

注意

说明:你可以根据需要,升级 ESXi 主机中的虚拟机,将原来的虚拟机硬件版本升级到最新的 11,这些可以根据需要设置,在此不再介绍。

被忽视的远程管理模块

四川 任绍坤

我公司各分厂的服务器统一在信息技术部机房托管,托管服务器的运维都是由各分厂的管理员或者委托外单位人员来负责,目前他们都使用 Windows 操作系

统的远程桌面功能进行远程管理和维护。这种远程管理方式在服务器的操作系统出现问题,或其他原因造成系统不可用时,就无法使用,托管服务器单位的服务器管

理员必须到机房来进行现场调试，一是不方便，二是由于信息技术部机房作为我公司的网管中心，设备多，一个机柜由多家单位的服务器共用，外单位人员进入机房，容易误操作碰到其他单位的服务器，给机房管理带来安全隐患。

如何解决这个问题呢？其实服务器厂商早就为我们提供了一种在服务器操作系统死机情况下仍能进行远程管理的功能模块，而这一功能又常常被忽视。现在的品牌服务器都自带了远程管理模块，例如 HP 服务器带有 ILO 模块，IBM 的 X 系列服务器的远程管理模块早期的叫做 RSA，现在叫做 IMM 模块。在信息技术部机房内托管的服务器 90% 以上都是 IBM 的 X 系列服务器，我们如果能利用这个曾经被我们忽视的服务器远程管理模块，就可以在系统死机状态下也可以轻松实现服务器的远程开关机，及时恢复故障服务器。而利用这一功能，只需要给每台服务器再连接一根网线到服务器管理口，并分配一个管理 IP 地址，无需其他额外的投入。

机房内服务器老款的以 IBM x460 为主，标配带有 RSAII 远程管理模块，新款的服务器以 IBM x3690、x3850 为主，带有 IMM 远程管理模块，这两种管理模块除了开始配置 IP 地址的方法稍有不同外，Web 管理界面几乎是一模一样的。下面就详细介绍使用远程管理模块实现远程管理的方法。

更改远程管理口的 IP 地址

IBM 服务器管理端口的默认 IP 地址为 192.168.70.125，我们首先就要修改管理口的 IP 地址，给每台服务器配置不同的管理 IP 地址。更改 IP 地址的方法有两种：方法一是通过开机按下 F1 键进入系统设置，配置 IP 地址。方法二是先通过 Web 登录 <http://192.168.70.125> 进入远程管理界面进行修改。RSAII 模块和 IMM 模块使用方法一修改 IP 地址稍有不同，详见下面的步骤。

RSA II 远程管理模块方法一修改 IP 地址步骤：

首先启动服务器，按 F1 进入 BIOS 设置，然后选择 Select Advanced Setup → RSA II Settings → 进入 DHCP control 到 Use Static IP → 填入 RSA II 的 IP address、subnet mask 和 gateway → 最后保存配置 Save Values and Reboot RSAII。

IMM 远程管理模块方法一修改 IP 地址步骤：

启动服务器按下 F1 键，进入 System Configuration

and Boot Management → 选择 System Settings → Integrated Management Module → Network Configuration → 在 DHCP Control 中选择 Static IP → 填入 IP address、subnet mask 和 gateway → 设置完后选择 Save Network Settings 保存，退出 Setup utility。

方法二修改 IP 地址步骤：

找一台笔记本电脑，配置 IP 地址为 192.168.70.1（这个地址可以任意指定，只要和服务器在一个网段即可），子网掩码：255.255.255.0，直接网线连接至服务器管理口，用 Web 方式登录 <http://192.168.70.125>，进入 IMM 管理界面进行修改。

更改远程管理默认用户 USERID 的密码，或者创建新用户

访问 IBM 远程管理模块默认用户名是 USERID，密码是 PASSWORD（0 是数字零而不是字母 O）。为了安全起见，用户在使用远程管理模块进行远程管理的时候，一定要修改一下密码。

用 Web 方式打开步骤一修改后的 IP 地址，在欢迎界面中，选择 timeout 值（此值为会话自动退出登录的时间）。如：我们可以选择 no timeout，点击 Continue 开始进入，浏览器将出现 System Status 页面（见图 1），然后选择 LoginProfiles，在这里可以修改 USERID 口令，或者新增远程用户，而且可以对不同的用户授予不同的远程管理权限。

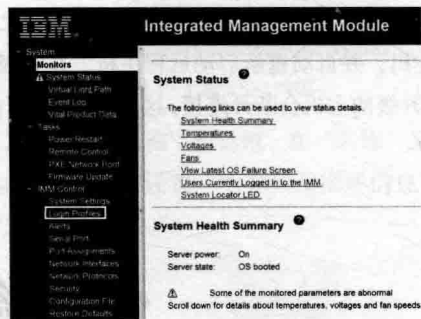


图 1 浏览器出现 System Status 页面

使用远程管理功能

远程管理功能分监视、任务、控制、分区四大功能模块。

在监视功能模块中，可以查看机器的日志、重要的

产品数据、光通路面板状态（IMM 模块有此功能）。任务功能模块中有我们最需要的功能——实现远程开关机，定时重启、远程控制，固件微码升级等功能。控制功能模块中有修改 IP 地址、创建用户、修改 USERID 口令、对不同用户进行远程管理授权等功能。通过这些功能，各单位的服务器管理员就可以远程查看服务器运行状态，在系统宕机时，远程重启服务器，快速修复故障，轻松实现服务器的远程管理。利用任务功能模块中的远程控制功能，还可以实现和 Windows 远程桌面类似的远程控制计算机的功能。

使用远程控制功能需在客户端计算机上安装好 Java 插件，在远程控制界面中有下载的连接，下载安装完成之后，需要进入 Java 控制面板配置，在例外站点列表中添加需要远程管理的 IP 列表（见图 2）。配置完成之后，在远程管理 Web 界面，选择用户连接到服务器终端方式：如果只允许一个用户连接到服务器终端，选择 Start Remote Control in Single User Mode；如允许多用户同时连接，选择 Start Remote Control in Multi-user Mode。远程连接成功的界面见图 3，然后就可以远程操作服务器了。

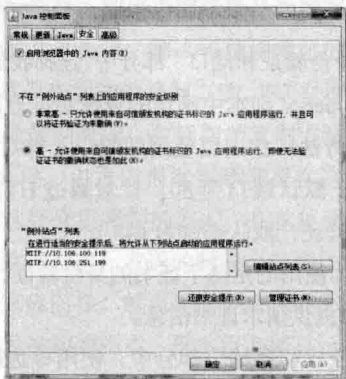


图 2 Java 控制面板



图 3 远程连接成功界面

注意

提示：有些服务器可能没有远程控制功能，这个功能需要 IBM Virtual Media Key 来实现，IBM3850 X5，3690 X5 服务器这个功能作为标配，但 IBM3850 M2 作为选件需要另外购买。没有此选件的服务器就需要配合 Windows 的远程桌面来实现远程控制功能。

经验总结

本文讲述的是使用曾经被忽视的服务器远程管理模块进行远程管理的一个小经验分享。如今购买的服务器、交换机、路由器等设备功能都很强大，但是很多功能没有充分利用，往往是这些被我们忽视的小功能却可以解决许多实际问题。借此机会，把这个远程管理的方法推荐给各位管理员来使用。

❖ 用复制功能实现灾备

上海 刘洁

单位有多台 Hyper-V 主机，每台 Hyper-V 主机上运行着多个虚拟机，那么如果有一台 Hyper-V 主机出现物

理故障宕机后，将导致所有虚拟机停止对外提供服务，或者有一台虚拟机突然出现宕机，怎样快速恢复正常对

外提供服务呢？我们可以使用 Windows Server 2012 或者 2012 R2 的 Hyper-V 新功能 Hyper-V 复制来实现虚拟机的副本，这样当一台 Hyper-V 主机或者虚拟机出现故障后，另外一台 Hyper-V 主机上因为有这些重要虚拟机的副本，我们启用副本就可以对外继续提供服务。这里给出了如何使用 Hyper-V 复制这个功能实现灾备。

测试环境

1. 两台使用 Hyper-V 角色运行 Windows Server 2012 或 Windows Server 2012 R2 的服务器用于 Hyper-V 的复制（这里主服务器命名 hype-v，副本服务器命名 hvback）要加入域中。

2. 服务器的地理位置，可以在物理上位于同一个位置，也可以位于完全不同的地理位置，主服务器和副本服务器在同一个防火墙后面，应该将防火墙配置为允许复制数据通过。

3. 主服务器和副本服务器在物理上共置而且位于同一防火墙后面，则可以使用内置 Kerberos 身份验证。

测试拓扑结构如图 1 所示。

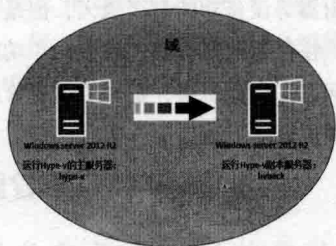


图 1 网络拓扑结构

步骤：配置副本服务器→启用复制→配置主服务器→测试部署→故障转移→总结。

配置副本服务器

1. 在 Hyper-V 管理器中，单击“操作”窗格中的“Hyper-V 设置”，在出现的对话框中，单击“复制配置”。在“详细信息”窗格中，选择“将计算机启用为副本服务器”，并选择“使用 Kerberos (HTTP)”端口保持 80 默认，在“授权和存储”选项下，选择“允许从任何经过身份验证的服务器中进行服务”，并指定副本的默认存储位置。可参考图 2 进行设置。



图 2 HYPER-V 的 Hyper-V 设置

2. 设置后向导会提示防火墙设置的相关警告，我们只需进入防火墙设置允许 Hyper-V 副本 HTTP 通过。

到此，副本服务器就配置好了，但是如果公司也配置了故障转移群集，副本服务器也是其中一部分，就需要考虑到故障转移群集了。接下来配置作为故障转移群集部分的副本服务器。

3. 在服务器管理器中，打开“故障转移群集管理器”。

4. 在左侧窗格中连接到群集，并在群集名称突出显示之后，在“详细信息”窗格的“导航”类别中单击“角色”。

5. 右键单击该角色，然后选择“复制设置”。

6. 在“详细信息”窗格中，选择“将此群集启用为副本服务器”。

7. 在“身份验证和端口”部分中，选择我们在步骤 1：准备部署 Hyper-V 副本中确定的身份验证方法。对于任一身份验证方法，指定要使用的端口（针对通过 HTTP 的 Kerberos，默认端口为 80。针对通过 HTTPS 的基于证书的身份验证，默认端口为 443）。

8. 如果你使用的是基于证书的身份验证，请单击“选择证书”，并提供请求证书信息。

9. 在“授权和存储”部分中，使用单选按钮指定是允许任何经过身份验证的（主）服务器将复制数据发送到此副本服务器，还是限制从特定主服务器接受数据。你可以使用通配符来限制从特定域接受服务器，而无需单独指定全部服务器（例如 *.contoso.com）。如果指定单个主服务器，则可以为每个服务器的副本数据指定单独存储位置，也可以使用“信任组”标记对其进行分组。

启用复制

1. 在主服务器 Hyper-V 管理器的“详细信息”窗格中，通过单击选中虚拟机，右键单击选定的虚拟机，然后指向“启用复制”。这将打开“启用复制”向导。在“指定副本服务器”页面的“副本服务器”框中，输入前面

步骤中配置的副本服务器的 NetBIOS 或完全限定的国际域名 (FQIDN)。开机下可以运行复制

2. 指定的副本服务器, 填写服务器名称 (见图 3)。

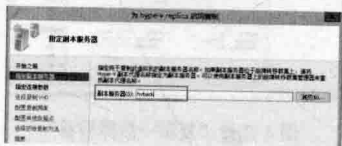


图 3 填写服务器名

3. 因为之前选择的是仅允许使用 Kerberos 身份验证 (HTTP), 如果网络带宽比较紧张, 建议勾选“压缩通过网络传输的数据”。

4. 选择复制 VHD, 选择要复制的 VHD, 也可以单独将虚机的 VHD 文件拷贝到副本服务器上, 这个根据实际情况而定。对于附加的 VHD 磁盘或者, 备份用的 VHD 可以不用勾选就不会复制到副本服务器上。

5. 根据需要配置复制频率, 这里笔者选择的是默认为每 5 分钟将更改发送到副本服务器。

6. 根据自己的实际情况配置恢复点, 在容灾级别不高, 可以“仅保留最新恢复点”。

7. “选择初始复制方法”下, 可以结合场景并根据实际情况进行选择。如果当前场景是局域网环境, 并且此时网络带宽并不拥挤, 那么可使用默认的“通过网络发送初始副本”作为初始复制方法, 并“立即启动复制”。或者设置启动复制时间, 包括初始复制方法, 就是前面说的 VHD 文件。也可以根据实际情况在这里通过网络复制, 或者选择介质复制的方式, 在这里我选择的是网络发送并且立即发送, 发送的时间也是蛮快的。

8. 点击完成向导, 就可以看到在发送数据了, 主服务器是正在发送初始副本, 副本服务器显示正在接收。

9. 发送接收完成之后, 可以看到副本服务器上多了虚拟机, 是关机的, 两台不能同时开启, 因为信息都是一样的, 包括角色、IP 地址等。同时, 也可以看到主服务器和副本服务器的信息, 以及上传同步的时间等。

10. 如果有需求, 副本服务器中的反向复制也可以将副本服务器变成主服务器。

配置主服务器

Hyper-V 副本通常将在主虚拟机上发生的更改发送到副本虚拟机, 但在故障转移后, 它可反向发送数据。通过执行此操作, 当你将操作从当前的主服务器故障转移到副本服务器时, 一旦主服务器重新联机可用, 即可

将复制方向从副本服务器更改回主服务器。通过此方式, 可以为目前用于处理虚拟机负载的副本服务器提供复制保护。

若要执行此操作, 只需使用用于副本服务器的 Hyper-V 上的相同设置即可。

测试部署

为了确保复制的虚拟机 (和其中运行的应用程序) 在副本服务器上如同在主服务器上一样正常运行, 我们可以随时执行测试故障转移。当执行测试故障转移时, 副本服务器上会创建一个临时的虚拟机, 在不中断进行中的复制的同时, 在测试虚拟机上测试任何应用程序。当结束测试时, 临时虚拟机将会删除。请注意:

1. 在故障转移后, 测试虚拟机不会连接到任何网络。如果必须执行需要网络的测试, 则用修改任何普通虚拟机设置的方式修改测试虚拟机的设置。

2. 若要成功执行测试故障转移, 必须针对至少一个虚拟机启用了复制, 并通过任何可用方法完成初始复制。若要使用最新恢复点以外的恢复点验证故障转移, 复制必须运行足够长的时间, 以便创建至少一个额外的恢复点。

(1) 访问副本服务器, 然后在 Hyper-V 管理器中, 右键单击要为其测试故障转移的虚拟机, 指向“复制...”, 然后指向“测试故障转移”。

(2) 选择要使用的恢复点, 这将创建和启动名称为“<virtual machine name>-Test”形式的虚拟机 (例如, “windows 10 test-Test”)。

(3) 可以在测试虚拟机上进行测试, 可以验证虚拟机的启动、暂停和停止, 以及虚拟机中的任何应用程序是否正常运行。

在结束测试之后, 通过选择“复制”选项下的“停止测试故障转移”放弃测试虚拟机。如果要删除同步复制的状态, 在复制下面点击删除复制即可。

测试故障转移

测试故障转移分为三种:

1. 计划内故障转移, 顾名思义也就是按照预先确定的计划来进行故障转移。该方式需要满足两个前提条件: 在初始故障转移前, 虚拟机必须关闭; 主服务器必须也启用复制功能, 并允许接收来自副本服务器的复制。

注意

要先关机才能执行故障转移。

成功转移后，可以看到在副本服务器上，转移的虚拟机正常运行，没有文件丢失。

2. 测试故障转移，在副本服务器上进行操作，允许在不中断当前持续的复制配置下，生成并启动一个新的用于测试用途的虚拟机。

3. 计划外故障转移，主服务器意外宕机时，我们可以在副本服务器上执行“故障转移”，将该虚拟机启动上线。

如图 4 所示，主服务器宕机，虚拟机管理服务也不可用，这时是属于计划外的故障转移。在副本服务器上，右键点击宕机的虚拟机，选择“复制→故障转移”，点击故障转移会出现一个选择使用的恢复点，点击“确认”，宕机的虚拟机就可以正常使用了。出现意外的虚拟机正常运行。



图 4 选择“复制→故障转移”

经验总结

通过 Windows Server 2012/2012 R2 下的 Hyper-V 复制功能，我们可以实现主服务器的整体灾备，同时也可定期复制，如果发生问题，快速在副本服务器上启动服务，复制的虚拟机角色和 IP 地址都不会发生变化。同时，也测试了故障转移的情况，可以实现需求。

通过 PE 查电脑 IP 地址

江西 张亮

目前，企业局域网中 PC 机 IP 地址分配方式主要有固定 IP 地址和自动分配两种，当企业采用固定 IP 地址分配，电脑由于软件故障而不能正常登录操作系统，多数人想到重装系统，如未提前备份 IP 信息，IP 地址信息默认存储 C 盘会丢失。下面介绍一种通过 U 盘或者光盘启动登录 PE 系统查看电脑 IP 地址的方法。

1. 通过光盘或者 U 盘一键启动，登录 PE 系统。

2. 进入 PE 系统中，点击“开始→运行”，输入命令 regedit，打开原系统的注册表。

3. 选中 HKEY_LOCAL_MACHINE 或者 HKEY_USERS。

4. 点击“文件→加载配置单元”（见图 1）。

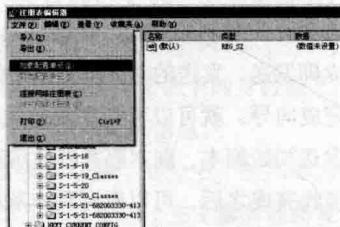


图 1 点击“加载配置单元”

5. 选择原系统文件夹路径：C:\WINDOWS\system32\config，有 5 个或者 6 个没有后缀的文件，分别是 default、SAM、SECURITY、software、system、userdiff。

6. 选择 System 文件并点击打开，提示输入一个项目名称，自定义即可（见图 2）。

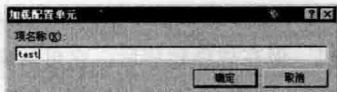


图 2 自定义项目名

7. 根据定义的加载配置单元名称, 按照以下路径查找手动配置的 IP 地址, 具体为: HKEY_LOCAL_MACHINE\test\ControlSe001t\Service\Tcpip\Parameters\

Interfaces\ (网卡对应的 ID 号) 下的 IPAddress 就是设置的 IP 地址。



Hyper-V 集群生成问题对策

山东 赵永华

Hyper-V Hosts 与 VMM Host Group

为生成 Hyper-V 集群, 需要通过系统组件工具 SCVMM 生成 VMM Host 组, 它是一个管理员单元, 可以分配共享型存储逻辑单元。如果 VMM Host 组没有分配逻辑单元, 那么在 Hyper-V 集群生成向导中就不会显示共享存储。在 Hyper-V 集群中, 应有两部甚至更多的 Hyper-V Hosts, 它们需要加入 VMM, 当然也就是 VMM Host 组的一部分。

例如, 笔者系统现有两台 Hyper-V Hosts, 分别命名为 Hyper-VHost1 和 Hyper-VHost2, 同时有一个名为 “Building2” 的 VMM Host 组, 此时就需要将这些 Hyper-V hosts 移至 VMM Host 组内, 因为 VMM 本身并不能对分布在不同 VMM Host 组内的 Hyper-V Hosts 进行集群化。此外, 通过 VMM 生成集群时还需要注意以下几点:

1. 安装 Failover Clustering 功能 (可选): 笔者在集群生成过程中曾经遇到出错, 具体信息是 “Error (25300) Cluster validation failed because of error: The server 'Server_Name' does not have the Failover Clustering feature installed. Use Server Manager to install the feature on this server”, 出错原因就是没有事先在 Hyper-V Hosts 上安装 Failover Clustering 功能。而且, Failover Clustering 要求 Hyper-V nodes 必须在同一个域内, 因为集群并不支持分布在不同域的节点。

2. Hyper-V Hosts 运行的操作系统必须配套, 比如, 集群的 Hyper-V 运行的是 Windows Server 2012 R2, 那么就必须相应地配以 VMM 2012 R2。

3. 激活 Multipath I/O (强制): 在 VMM 中为访问共享型存储, 必须要对每台 Hyper-V 主机用 Server

Manager 进行 Multipath I/O (MPIO) 安装, 因为当我们将来 Hyper-V 主机添加到 VMM 时, SCVMM 并不会自动添加 MPIO 功能。当我们将来 Hyper-V 主机添加进 VMM 主机组时, 如果 Multipath I/O 功能尚未安装, 就会看到 VMM 显示警告信息。

4. 安装 Microsoft iSCSI Initiator (可选): 如果将来 iSCSI SAN 作为共享存储, 那么一定要确保集群中每台 Hyper-V 主机应当安装并运行有 iSCSI 初始化服务, 在集群生成过程中, VMM 会调用该服务在 Hyper-V 节点上会自动配置此共享型存储。

Hyper-V 共享型存储

既然 Hyper-V Cluster 针对的是共享型存储, 那么在生成 Hyper-V 集群之前, 就需要准备好共享型存储。VMM 支持连接设备类型包括有 iSCSI、Fibre Channel SANS 及相关存储阵列, 由其构成的存储池可供 Hyper-V 主机使用。鉴于这里的共享型存储是由 SCVMM 管理, 需要强调以下几点:

1. 有关共享存储阵列需要在 Virtual Machine Manager 中的 Fabric Workspace 进行添加组合, 具体而言, 即打开 Virtual Machine Manager, 进入 Fabric Workspace 后, 右击节点 “Storage” 并点击 “Add Storage Devices”。

2. 存储池及其逻辑单元只能在 VMM Host 组进行分配, 所分配的存储池只能供 VMM 调用, 所分配的逻辑单元则既能供集群也能供 VM 调用。有时可以不必对存储池进行分配, 但逻辑单元必须在有关 VMM Host 组内进行分配, 如此, 集群生成向导才能显示可用的逻辑单元。逻辑单元的生成, 来自 Fabric Workspace 中的

“Create Logical Units”按钮，当生成一组逻辑单元后，右点 Hyper-V 节点中的 VMM Host 组便有菜单“Allocate Logical Units”。由存储共享池生成的逻辑单元并非一定要分配给特定的 Hyper-V 主机，而 Hyper-V 集群生成向导只能检测到那些没有分配给任何 Hyper-V 主机的逻辑单元。

3. 当我们使用 Hyper-V 主机所管理的共享型存储时，需要确认由某台 Hyper-V 主机所生成的逻辑单元一定是 NTFS 分区格式，此乃 Failover Cluster Manager 建立 Hyper-V 集群所要求的。

Hyper-V 主机的网络化需求

当通过 VMM 生成 Hyper-V 集群时，Hyper-V Cluster 向导工具会适时出现让我们去分配 IP 地址的页面，但是否会看到该页面取决于以下几个条件：

1. 如果在每台 Hyper-V 主机上正在采用静态 IP 配置方式，那么一定要确保在所有 Hyper-V 主机上至少有一部物理的网络适配器属于相同的 IP 子网，而且要使用默认网关。

2. 如果将 Hyper-V 主机配置为从 DHCP Server 获取 IP，那么集群生成向导并不会向我们提供为集群分配 IP 地址的页面。虽然 Windows Server 2012 及其之后的操作系统支持该方式，但此时集群生成向导会自动从 DHCP Server 获取有效的 IP 地址，但并不会出现让我们提供 IP 地址的页面。

3. Hyper-V 集群生成向导支持在每台 Hyper-V 主机上自动生成虚拟交换机 Virtual Switch，但此举并非必须，也可以之前就完成，关键是调用 VM Network 的物理网络适配器一定来自有效的 Hyper-V 主机。

用 Virtual Machine Manager 生成 Hyper-V 集群

为启动 Create Cluster Wizard，我们进入 VMM Console，转到 Fabric 后点击“Create”按钮然后选择“Hyper-V Cluster”（见图 1）。

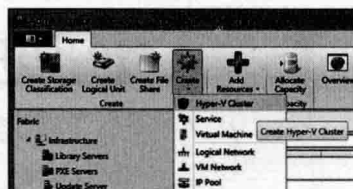


图 1 选择“Hyper-V Cluster”

然后进入“Create Cluster Wizard”窗口，点击“Hyper-V Cluster”按钮后由以下步骤建立 Hyper-V 集群。

1. 分配 Cluster Name：在 General Tab 栏目内输入集群名称以及认证等信息。

2. 选择 Hyper-V Nodes：选择 Host Group，其包含有属于 Hyper-V 集群的 Hyper-V 节点，此时所选的 Hyper-V 节点不能来自不同的 VMM 机组。

3. 为集群分配 IP 地址，这里需要注意的是如何避免 IP 页面消失的情况发生。

4. 选择共享型硬盘，我们为 Hyper-V 集群所选硬盘包括两类，即 Witness Disk 与 Cluster Data disk，Create Cluster Wizard 会自动将 Witness Disk 选为硬盘，而 Cluster Data 硬盘用于存储虚拟机文件如 XML 和 VHD/VHDX。

5. 分配虚拟交换机，即在目标 Hyper-V 节点上选择逻辑网络作为虚拟交换机，VMM 会在所有 Hyper-V 节点自动生成虚拟交换机。

6. Hyper-V 集群的配置，在 Hyper-V Cluster 属性页面有多个配置栏目，涉及可用存储、文件共享存储以及虚拟交换机等。



ARP 代理解决地址重叠



金华 盛建平

网络结构

某集团公司的分部有多个网点，先期组网整个分部在同一网段内，即分部 Web 服务器、网点主机地址全部在总部分配的 10.0.0.0/20 地址段内，如图 1 所示的虚线左下部分。

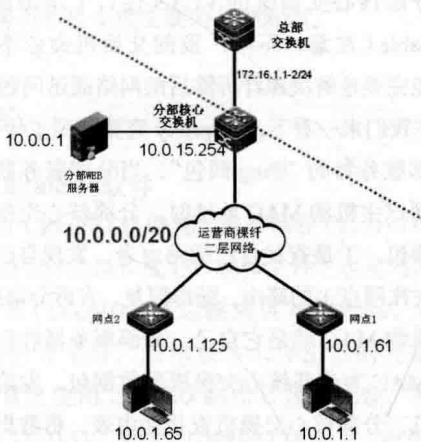


图 1 网络拓扑结构

该种组网方式虽简单，但却存在诸多问题，如同网段内主机过多、MAC 地址表过大、广播对网络影响大、网络性能低、ARP 欺骗频繁等。为彻底解决上述问题，拟对网络地址进行改造，对总部分配的地址组子网化，每个网点单独的网络，分配 64 个地址。地址分配表如表 1 所示。

改造计划

整个网络改造计划如下：

1. 因地址是总部统一分配的，所以新规划的地址与原地址存在包含关系，需新增一台交换机，用作网络改造后的网点的接入网关，新增交换机与原分部核心交换机之间增加三层连接，新增交换机默认路由指向原分部核心交换机。
2. 每个网点新增一条专线，并规划独立的 VLAN，网关设在新增交换机上。
3. 修改网点交换机及网点主机的掩码及网关，IP 地址不变。
4. 在原核心交换机上，新增改造后网点的路由，指向新增交换机。
5. 测试成功后，拆除原裸纤。
6. 分部 Web 服务器等需在所有网点改造完成后再实施掩码与网关的变更，否则未改造的网点会网络不通。

注：该种改造方法可以逐个网点改造，且网点及中心 IP 地址本身不变（仅变更掩码及网关），对应用配置无影响。

网点 1 改造过程中的拓扑结构如图 2 所示。

表 1 地址分配表

网点	VLAN 号	网络号	网关	网点交换机管理 IP	主机地址
分部中心	200	10.0.0.0/24	10.0.0.254		10.0.0.1-10.0.0.253
网点 1	201	10.0.1.0/26	10.0.1.62	10.0.1.61	10.0.1.1-10.0.1.60
网点 2	202	10.0.1.64/26	10.0.1.126	10.0.1.125	10.0.1.65-10.0.1.124
网点 n	203

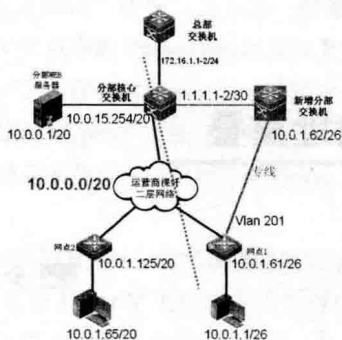


图 2 网络改造结构

故障现象

根据上述步骤实施网点 1 的网络变更，改造后发现网点 1 的主机 10.0.1.1（以下简称网点主机）能 Ping 通分部 Web 服务器 10.0.0.1（以下简称分部服务器），但将原裸纤拆除后，却不能 Ping 通分部服务器。为什么会这样呢？在 Ping 通的情况下，裸纤承载什么作用呢？

故障分析

我们来分析一下，网点主机 IP 为 10.0.1.1，掩码为 255.255.255.192，当它发起 Ping 分部服务器 10.0.0.1 时，经比较，发现目标主机为非本网段主机，于是将“Ping 包”发给网关（新增交换机）处理，新增交换机查找路表，将“Ping 包”发给分部核心交换机处理，分部核心交换机发现目标主机在本交换机的一个直连接口上，于是直接发给分部服务器。

当然，通讯是双向的，当分部服务器收到网点主机的“Ping 包”时，它会怎么处理呢？分部服务器的地址为 10.0.0.1，掩码为 255.255.240.0，经比较，发现目标主机 10.0.1.1 与本机为同网段的，就会发广播包查它的 MAC 地址，而裸纤此时是正常的，网点主机通过裸纤返回 MAC 地址给分部服务器，“Ping 回包”就通过裸纤直接回传给网点 PC。由此可以看出，数据的往返

路径是不一致的，上行走新增的专线，下行还是走原来的裸纤，这样当裸纤中断后，网络自然就不通了。

问题似乎无解了，从分部服务器这端来说，因为掩码问题，认为改造后网点主机跟它是同网段的，自然不会将数据包扔给网关处理，这样裸纤就不能拆除，网络改造宣布失败。

故障解决

有没有办法让分部服务器的“Ping 回包”发给分部核心交换机呢？因为只有它才能将改造后网点的数据包发往正确的目的地。这时，ARP 代理闪了一下，能否用 ARP 代理解决分部服务器的 MAC 广播呢？答案是肯定的。

在分部核心交换机的 VLAN 接口上增加配置 `arp-proxy enable`（注意，不同厂商的交换机命令不一样），这样就能完美地解决裸纤拆除后的网络通讯问题。

现在我们来一看下，`arp-proxy` 究竟起到了什么作用。还是分部服务器的“Ping 回包”，当分部服务器通过广播查找网点主机的 MAC 地址时，分部核心交换机收到了该广播包，于是查找自己的路由表，发现自己的路由表中有去往网点 1 的路由，随即回复，告诉分部服务器，网点主机的 MAC 就是它自己。分部服务器收到后，构造目标 MAC 为分部核心交换机的数据包，发给分部核心交换机，分部核心交换机查找路由表，将数据发给新增交换机，这样将“Ping 回包”通过新专线返回给网点主机。至此，网络改造得以继续进行。

经验总结

这次碰到的问题，虽然解决起来只有一条命令，但却需要平时多多了解网络技术。“厚积而薄发”，只有平时注重网络知识的积累，才能在碰到问题时信手拈来，快速地解决网络中碰到的问题。



服务器操作系统巧安装

福建 邱旭华

相对于普通 PC，在服务器上安装操作系统要麻烦得多。因为服务器的硬盘通常都挂载在阵列卡上，在安装操作系统过程中需要按 F6 键通过软驱加载阵列卡驱动，否则安装程序会因找不到硬盘使安装终止。遗憾的是，很多服务器都没有配置软驱，有的服务器甚至连光驱也没有……下面我们将介绍如何通过各种软件组合，解决服务器操作系统安装的各种麻烦。

准备篇

1. UltraISO 软件

通过 UltraISO 软碟通，将存储在 CD/DVD-ROM 或硬盘上的文件的制作成 ISO 镜像文件，也可写入 ISO 映像文件到 CD/DVD。可以逐扇区复制光盘，提取 CD/DVD 的引导文件，制作包含引导信息的完整映像文件。可直接使用 UltraISO 制作 U 盘启动盘，系统引导光盘（CD/DVD）制作。UltraISO 涵盖了六种写入类型：USB-HDD、USB-ZIP、USB-HDD+、USB-ZIP+、USB-HDD+ v2、USB-HDD+ v2，根据不同兼容性，满足启动盘的制作要求。

2. nLite 软件

nLite 是由 MSFN (Microsoft Software Forum Network) 会员 nuhi 编写的免费软件，这个软件可以为您所定制的 Windows 安装文件集成 Service Pack 和 Windows 安全更新程序，还可以集成常用的应用软件（包括 DirectX、.Net Framework、软件整合包、桌面主题和驱动程序等），并且可以移除 Windows 安装组件里面你认为不需要使用的组件，以减少 Windows 安装文件的容量，而且还可以优化调整注册表、更改系统服务设置、进行 Windows 无人参与安装以及创建可引导的 ISO 光盘镜像等功能。

3. WinCAB 软件

CAB 格式文件是 Microsoft 制定的压缩包格式，常

用于软件的安装程序。本文中我们需要用 WinCAB 软件来打开操作系统安装文件中的 CAB 格式文件，修改部分参数。

4. 基于 WinPE 的 U 盘启动盘制作软件

Windows PE 是 Windows Preinstallation Environment (Windows PE) Windows 预安装环境，是带有有限服务的最小 Win32 子系统，基于以保护模式运行的 Windows XP Professional 及以上内核。它包括运行 Windows 安装程序及脚本、连接网络共享、自动化基本过程以及执行硬件验证所需的最小功能。当前基于 Windows PE 基础开发的 U 盘启动盘制作软件很多，本文以老毛桃装机版为例进行介绍。

5. 准备阵列卡驱动

如果没有现成的阵列卡驱动程序，我们首先得知道阵列卡的型号。可以通过装机资料看是否能够找到阵列卡型号，也可以通过开机中按相应阵列卡配置的快捷键进入阵列卡 BIOS 了解阵列卡型号。确定了阵列卡型号以后，我们再进入服务器厂商官网或阵列卡厂商官网下载操作系统对应版本的驱动程序。

6. 准备 ISO 格式的操作系统

如果有操作系统安装光盘，我们可以通过 UltraISO 软件生成 ISO 格式文件，没有的话，就只有上网下载一个了。

方案篇

对于服务器管理员来说，往往需要维护各种不同品牌不同阵列卡配置的多台服务器。在维护过程中，都会碰到以下一些问题：服务器厂商没有提供系统安装引导光盘；软盘或光盘介质失效；服务器没有软驱、光驱或软驱、光驱失效；即使软硬件都齐全，但要保管一堆的配套软盘和光盘很麻烦。如图 1 提供的解决方案中，我们完全把软驱抛弃，做到一个 ISO 文件通吃所有服务器的操作系统安装。

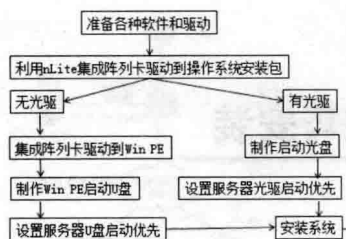


图 1 操作系统安装解决方案

1. 利用 UltraISO 软件把操作系统 ISO 格式文件全部提取到硬盘中“E:\win2003”下，把阵列卡驱动放置在“E:\drivers”，利用 nLite 软件把阵列卡驱动集成到“E:\win2003”中。nLite 软件提供在集成驱动之后自动生成新的 ISO 镜像文件功能，当然我们也可以集成后利用 UltraISO 软件把“E:\win2003”下文件打包为“win2003new.iso”备用（我们可以把所有要维护的服务器阵列卡驱动一次性集成，这样就可以实现一个 ISO 文件通吃所有服务器）。

2. 如果服务器有光驱，只需要利用 UltraISO 软件把“win2003new.iso”刻录到光盘，进入服务器 BIOS 设置光驱优先引导，就可以开始安装操作系统了。安装过程中程序自动识别硬盘，分出一块空间安装系统即可，其余空间可以等安装完毕再分配。如果没有光驱，则需要进行后续操作。

3. 通过 WinCAB 和 UltraISO 软件把驱动程序集成到老毛桃 Win PE 中，最终生成包含阵列卡驱动的“WinPEnew.iso”。

4. 利用老毛桃装机版提供的“ISO 模式”功能，把选择“WinPEnew.iso”文件生成 Win PE 启动 U 盘，再把“win2003new.iso”文件拷贝到 U 盘的 ISO 文件夹下。

5. 插入启动 U 盘，设置服务器 BIOS 从 U 盘引导加载老毛桃 Win PE，因为集成了阵列卡驱动，我们在 PE 里直接对硬盘分区，再利用 PE 自带的系统安装器安装 U 盘 ISO 文件夹下的“win2003new.iso”。

制作篇

在制作篇中我们重点对方案篇中关键的操作步骤进行讲解，其他操作请自行查找资料。

1. UltraISO 的使用

打开 ISO 文件：选择“文件”菜单下“打开”，可以打开 ISO 格式的操作系统安装包。

提取 ISO 中的文件：为了修改 ISO 格式的光盘镜像

文件中的某个文件，我们需要进行提取。方法是先选择需要提取的文件或文件夹，在执行“操作”菜单下“提取”。

添加文件或文件夹：在修改完提取出来的文件后，执行“操作”菜单下“添加文件”或“添加目录”把修改后的文件或文件夹添加进来，覆盖原来的文件或文件夹。覆盖完成后，执行“文件”菜单下的“另存为”进行保存修改结果。

新建 ISO 文件：执行“文件”菜单下“新建”，然后把要添加的文件之间拖拽到软件右窗格中，再执行“文件”菜单下的“保存”即可。此操作在本文中用于打包“E:\win2003”下集成驱动后的的安装文件。

刻录光盘映像：对操心系统 ISO 文件，可以通过“工具”菜单下“刻录光盘映像”，把集成了驱动的操作系统安装文件刻写到光盘。

2. 使用 nLite 集成阵列卡驱动

启动 nLite，选择语言为中文，点击“前进”，在“请选择 Windows 安装文件所在位置”界面中点击“浏览”，选择操作系统 ISO 格式文件解压后的文件夹“E:\win2003”，界面中将显示操作系统的相关信息。

跳过“预设”操作，进入“任务选择”界面。选择“驱动程序”和“可引导 ISO 镜像”两个任务。点击“前进”，进入下一步任务。

在“驱动程序”界面中点击“插入”，选择要插入的驱动程序。这一步我们可以同时插入多个驱动程序，做到一个 ISO 镜像识别你想要识别的所有阵列卡。

如果在第二步没有选择“可引导 ISO 镜像”，也可以在集成完毕后利用 UltraISO 软件把修改后的“E:\win2003”打包成“win2003new.iso”。

3. 集成阵列卡驱动到 WinPE

第一步：在“E:\drivers”文件夹下找到扩展名为 SYS 的驱动文件，比如名称为“XXXSATA.SYS”，把它用 WinCAB 打包成为 CAB 文件，然后把这个 CAB 重命名为“XXXSATA.SY_”。另外也可以直接利用 nLite 软件集成驱动后自动打包好的驱动程序文件，位置在“E:\win2003\i386\ndrv”文件夹中。

第二步：生成 ISO 格式的老毛桃 PE 文件。启动老毛桃装机版，在“模式类别”中选择“ISO”模式；在“ISO 生成”框中点击“浏览”，设定生成的 ISO 文件位置，我们设置生成到 E 盘；点击“一键生成 ISO 文件”，生成完毕，E 盘下将生成一个名为“LMT.ISO”的文件，这是老毛桃 PE 的 ISO 格式光盘镜像文件。

第三步：利用 UltraISO 软件打开“E:\LMT.ISO”，

找到“LMT3.IS_”，拖拽到E盘。“LMT3.IS_”是WinPE内核打包后的文件，直接把扩展名改为CAB。利用WinCAB软件打开“LMT3.CAB”，可以发现里面是一个名为“LMT3.ISO”的文件，把解压到E盘根目录。

第四步：利用UltraISO软件打开“LMT3.ISO”，找到文件“TXTSETUP.SI_”，拖拽到E盘根目录备用。再把第一步打包好的“XXXSATA.SY_”添加到“LMT3.ISO”的“SYSTEM32\DRIVERS”文件夹下。不要关闭UltraISO软件，因为后面我们需要把修改后的“TXTSETUP.SI_”覆盖进来。

第五步：修改“TXTSETUP.SI_”。它是Windows预安装环境配置文件，我们需要修改其中的四个部分的参数，分别位于[SCSI]、[SCSI.Load]、[HardwareIdsDatabase]和[SourceDisksFiles]字段。

把“TXTSETUP.SI_”改名为“TXTSETUP.CAB”，利用WinCAB解压得到“TXTSETUP.SIF”，利用记事本打开，在上述四个部分添加相应参数。

查找[SCSI]字段，在其下添加XXXSATA=”XXX SATA CONTROLLER”。它的作用是在Windows预安装环境加载的时候，显示“正在加载XXX驱动”字样。

查找[SCSI.Load]字段，在其下添加XXXSATA=XXXSATA.SYS，它的作用是加载驱动，此处加载的SYS文件，而我们第一步生成的是SI_文件，这不是错误，其实程序自己知道分析解压缩，只要保持名字的一致性就行了。

查找[HardwareIdsDatabase]字段，在其下添加PCI\VEN_105A&DEV_3373=”XXXSATA”。代码中PCI后面的数字编号根据阵列卡不同而不同，它的作用是标

识硬件。这串数字在驱动文件的INF或OEM文件里面可以找到。

查找[SourceDisksFiles]字段，在其下添加XXXSATA.sys=1,,,,,4_,4,1,,1,4。

TXTSETUP预安装配置文件里还有很多强大的参数，深度定制能打造出更个性化的PE系统。

第六步：利用WinCAB软件把修改后的“TXTSETUP.SIF”重新打包为CAB格式文件，再把这个CAB文件改名为“TXTSETUP.SI_”，最后利用UltraISO软件在第四步所说的“LMT3.ISO”中添加并替换原来的SI_文件。

第七步：对修改后的“LMT3.ISO”文件利用WinCAB重新打包为“LMT3.CAB”，再改名为“LMT3.IS_”。利用UltraISO打开“LMT.ISO”，添加并替换掉原来的“LMT3.IS_”，最后把“LMT.ISO”另存为“WinPEnew.iso”。

维护篇

如方案篇所述，服务器操作系统的维护中存在各种问题，因此在日常维护中，我们要重视驱动程序的备份。利用本文介绍的方法把阵列卡驱动、网卡驱动等重要的驱动程序备份并集成到操作系统安装文件中，需要的时候就可以快速安装一个全新的操作系统。另外我们也可以利用Ghost工具把正常运行的服务器系统盘备份起来，一旦出现问题，利用装有WinPE的U盘启动盘，可以快速恢复系统和业务，这样就不用再在恢复系统后再逐个安装原来的业务系统。



部署高可靠性ACS主备机

湖北 张亚舟

笔者所在单位下设9个县级单位，路由器设备20余台、交换机设备30余台，作为单位的网络管理员，肩负着保障全部网络设备正常运行的职责。为了更好地管理这些网络设备，我们部署了2台Cisco Secure

Access Control System服务器（简称ACS服务器），2台ACS服务器以主备方式部署、数据库同步复制，切实提高ACS服务器故障切换的高可靠性。

ACS客户端，如路由器、交换机及防火墙等，必须

在配置中指定两个或多个 AAA 服务器地址，AAA 客户端会按配置中列出的 AAA 服务器顺序，逐个尝试通信。如果在配置的超时时间内无法连接第一个服务器，则会尝试下一个，以此类推。如果客户端收到第一个 AAA 服务器的应答，则不会尝试连接第二个服务器，且不能强制 AAA 客户端首先连接第二个服务器，这样才可以完全实现冗余高可靠性部署。

配置 ACS 主机

1. 显示 ACS 内部数据库同步复制菜单

ACS internal database Replication（内部数据库同步复制）功能有可能是隐藏状态（缺省是隐藏的），需要修改 Interface Configuration 设置，来调出内部数据库同步复制功能，方法如下：

选择 Interface Configuration → Advanced Options，勾选 Distributed System Settings 和 ACS internal database Replication，后者需要前者支持。

2. 添加 ACS 备机

ACS 内部数据库同步可以支持多台备机，必须事先在 ACS 主机的 AAA 服务器列表中添加所有的备机，方法如下：

（1）如果已经启用 NDG：

选择 Network Configuration，选择 Network Device Groups 中 Not Assigned。点击 AAA Servers 列表下方的 Add Entry 按钮，输入 ACS 备机的名称、IP 地址及相应的密钥，然后点击 Submit+Apply 按钮。

（2）如果未启用 NDG：

直接选择 Network Configuration，然后点击右边 AAA Servers 列表下方的 Add Entry 按钮，在打开的 Add AAA Server 页面中输入相应的信息后，按 Submit+Apply 即可。

3. 设置 ACS 内部数据库同步复制

选择 System Configuration → ACS Internal Database Replication，确认 ACS 主机上同步组件勾选情况如图 1 所示。在 Outbound Replication 表项下，选择相应的同步时间表计划类型，ACS 主机上可以选用四种中任何一种。在 Partners 表项中，在左边 AAA Servers 列表框中选择相应的备机，然后点击 → 按钮，添加到右边的 Replication 列表框中，最后按 Submit 按钮提交设置。

配置 ACS 备机

1. 显示 ACS 内部数据库同步复制菜单

方法同 1，显示 ACS 内部数据库同步复制菜单。

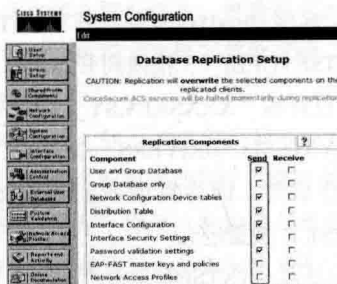


图 1 ACS 主机数据库同步复制设置图

2. 添加 ACS 主机

要完成数据库同步复制，必须在 ACS 备机的 AAA 服务器列表中添加 ACS 主机，方法如下：

（1）如果已经启用 NDG：

选择 Network Configuration，选择 Network Device Groups 中的 Not Assigned。点击 AAA Servers 列表下方的 Add Entry 按钮。输入 ACS 主机的名称、IP 地址及相应的密钥，然后点击 Submit+Apply 按钮。

（2）如果未启用 NDG：

直接选择 Network Configuration，然后点击右边 AAA Servers 列表下方的 Add Entry 按钮，在打开的 Add AAA Server 页面中输入相应的信息后，按 Submit+Apply 即可。

3. 设置 ACS 内部数据库同步复制

选择 System Configuration → ACS Internal Database Replication，确认 ACS 备机上同步组件勾选情况（见图 2）。在 Outbound Replication 表项下，选择相应的同步时间表计划类型。注意：ACS 备机上只能选择默认的 Manually 方式。直接按 Submit 按钮提交配置。注意：ACS 内部数据库同步不支持双向同步复制，因此要确保备机上没有将 ACS 主机添加到 Replication 列表框中。



图 2 ACS 备机数据库同步复制设置图

同步数据库

数据库同步必须由 ACS 主机发起，备机只能被动接收数据库信息。

1. 手动启动数据库同步

在 ACS 主机上选择 System Configuration → ACS Internal Database Replication，然后点击 Replicate Now 按钮，手动向备机同步复制数据库。

2. 验证数据库同步状态

主备数据库同步启动后，可以在 ACS 主机上查看相关报表来验证数据库同步是否成功，方法如下：

选择 Reports and Activity → Database Replication，打开数据库同步状态报表。点击右边框架页面中的 Database Replication active.csv。可以看到 text-message 列中的相关信息，获取当前数据库同步状况。

3. 数据库同步复制注意事项

ACS 主备机数据库同步复制使用的目标端口 TCP:2000。确认操作系统中网卡的防火墙功能已关闭。启用 Java 和 JavaScript，禁用 HTTP 代理。确保可以使用 TCP:2002 远程访问 ACS 用户界面。

让 View 6.1 支持 XP

河北 王春海

如果你的 Horizon 6.2 是从 6.0 的版本升级而来，则配置使用 Windows XP 的 View 桌面没有任何问题，但如果你的 Horizon 6.1 或 6.2 是全新安装，则在添加 Windows XP 的桌面池后，在置备 Windows XP 的桌面时，会出现 “No Network communication between the View Agent and Connection Server. Please verify that the virtual desktop can ping the Connection Server via the FQDN” 的错误。

出现这一问题的原因，是 Horizon 6.1（或 6.2 版本）默认将 Message Security mode 设置为 Enhanced，而且无法通过 View Administrator 控制台界面或者 vdmutil 进行更改。

而升级到 Horizon 6.2 的连接服务器，在 “View 配置→全局设置”，在安全性设置中，该项如图 1 所示。

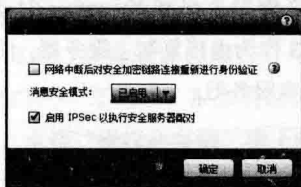


图 1 升级到 Horizon 6.2 版本连接服务器默认项

在全新安装的 Horizon 6.1（或 6.2）连接服务器中，

将此项改为 “已启用” 即可。解决方法是使用 adsiedit.msc 进行更改。

在下面的操作中，View 6.2 是全新安装，其计算机名称为 vcs，加入到名为 heuet.com 的域，计算机属性如图 2 所示。



图 2 示例 View 连接服务器计算机名称

1. 以管理员的身份登录到 Horizon View 6.2 连接服务器，打开 “运行” 对话框，输入 adsiedit.msc，然后回车键。

2. 打开 “ADSI 编辑器” 之后，右击 ADSI 编辑器，在弹出的对话框中选择 “连接到”。

3. 在弹出的 “连接设置” 对话框中，在 “连接点” 处单击 “选择或键入可分辨名称或命名上下文”，并在栏目中输入 DC=vdi，DC 搜索=vmware，DC=int（英文输入，此名称与你的 Active Directory 域名无关），

在“计算机”处单击“选择或键入域或服务器”，输入 localhost:389，或者输入你的计算机名称及端口号，例如本示例中为 vcs.heuet.com:389，之后单击“确定”按钮。

4. 返回到 ADSI 编辑器，依次展开 OU=Properties → OU=Global，然后双击右侧的 CN=Common。

5. 将 CN=Common 里面的 pae-MsgSecMode 值由默认的 ENHANCED 改为 ON，注意，是大写的字母 O，不是数字 0。

6. 右击“默认命名上下文”，在弹出的快捷菜单中

选择“现在更新架构”。

7. 打开“服务”，重新启动 VMware Horizon View 连接服务器。

8. 再次登录 View Administrator，在“View 配置→全局设置”，编辑“安全性”，查看，此时默认值已改为“已启用”，并且该项可选择。

经过这样配置，Horizon 6.1（或 6.2）即可以支持安装了 View Agent 6.02 版本的 XP 或 Vista 的 View 桌面。

快速备份与迁移虚拟机

天津 武金刚

当我们在宿主主机上创建多个 Hyper-V 虚拟机时，可以非常方便地对多个虚拟机进行维护。可是，任何系统都不是高枕无忧的，虚拟机也不例外，因此确保虚拟系统中的数据安全，也是网管员首要考虑的问题。其实，虚拟机数据备份方法很多，如使用 SMB 共享存储的实时迁移、Hyper-V over SMB、共享存储的实时迁移等。但是这些方法不仅设置上有些麻烦，还需要一些设备的投入，对于学校或小型企业来说要求有些过高。在 Hyper-V 3.0 中，提供了一个复制功能，使用这个功能，操作和设置上都比较容易。

Hyper-V 复制，即 Hyper-V Replica，也称之为 Hyper-V 副本，是一种异步虚拟机复制技术，基于 HTTP 协议进行传输，所以它也非常适合应用在广域网环境中。在设计上，Hyper-V 复制主要用于商业连续性和灾难恢复场景。因为不需要任何共享存储，所以该技术可用于任何服务器、网络或存储供应商的设备。下面我们就来了解一下通过“Hyper-V 复制”来备份当前的虚拟机。

准备工作

我首先虚拟一个单位网络场景，并在该场景下完成 Hyper-V 虚拟机的复制（见图 1）。在该局域网内，可以

将虚拟主机 A 中的虚拟系统复制到虚拟主机 B 中。下面就来看一下操作过程。

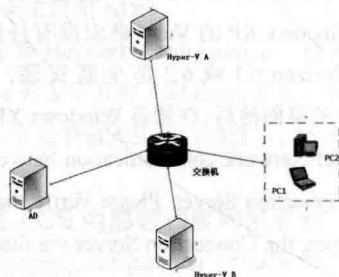


图 1 域环境工作模式

在此值得一提的是，Hyper-V 复制是依赖于域环境的，也就是说复制到的两个虚拟主机需要加入到同一个域中才能实现此功能。域的创建、添加过程本文不再详细介绍。

在实际操作中，为了不让读者混淆，我们分别准备了 Xy-server-03 虚拟主机和 Xy-server-04 虚拟主机，其中 Xy-server-03 作为虚拟复制主服务器，而 Xy-server-04 服务器作为副本服务器。

开启 Hyper-V 复制功能

使用 Hyper-V 的复制功能备份系统前，首先要在需要备份的 Hyper-V 服务器（在此以 xy-server-03 服务器

为例)上启用 Hyper-V 的复制功能。

1. 启用 Kerberos 协议

使用复制功能时,需要在 Hyper-V 角色中启用 Kerberos 协议。登录到 xy-server-03 服务器,在“服务器管理器”中单击“添加角色和功能”,随后在弹出的添加角色列表中勾选“Hyper-V”角色,在添加向导中勾选“包括管理工具”选项。

随后,单击“添加工具”,接着在“迁移”界面中勾选“允许此服务器发送和接收虚拟机的实时迁移”复选框,并在下面的身份协议中勾选“使用 Kerberos”协议,并单击“下一步”默认安装即可(见图 2)。

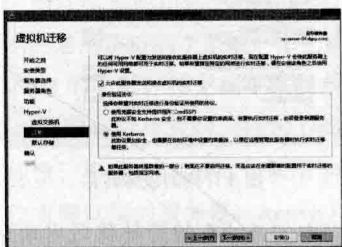


图 2 启用“使用 Kerberos”协议

2. 配置 Hyper-V 的复制服务器

启动 Hyper-V 管理器,右键单击管理器列表中的服务器名称,在弹出的右键菜单中选择“Hyper-V 设置”命令。

在弹出的“Hyper-V 设置”界面中,单击左侧的“复制配置”,打开“复制配置”界面(见图 3)。

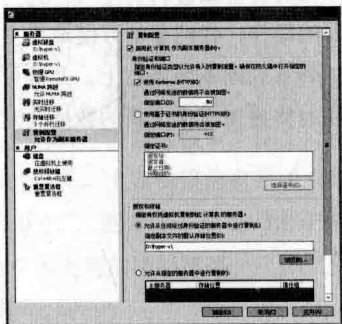


图 3 复制配置界面

在此勾选“启用此计算机作为副本服务器”复选框,并在下面的“身份验证和端口”项中勾选“使用 Kerberos (HTTP)”复选框,根据需要更改其指定的端口号。接着,点选“授权和存储”项下的“允许从任何经过身份验证的服务器中进行复制”选项,并在下面的“指定副本文件的默认存储位置”项中选择副本文件存储文件夹,随后单击“确定”按钮退出设置。

如果我们想指定服务器作为副本虚拟机服务器,在

此需要点选下面的“允许从指定的服务器中进行备份”选项,并单击下面的“添加”按钮,打开“添加授权条目”界面。

在指定主服务器对话框中,输入接受副本文件服务器名称;在“指定副本文件的默认存储位置”项中输入副本文件保存的文件夹;在“指定信任组”文本框中输入两个服务器所在的域名地址,设置后单击“确定”按钮即可。

按照上面的方式,需要将另一台虚拟机主机复制功能开启。虚拟服务开启后,在 Windows Server 2012 系统自带的防火墙中,将 Hyper-V 复制功能允许进行通信。

开始备份副本

通过上面的设置后,我们已经在主复制服务器上对 Hyper-V 的复制功能进行了配置。下面就可以在主服务器上启用复制功能了。

启用时,打开虚拟机主服务器的 Hyper-V 管理界面,在虚拟机列表中右键单击需要备份的虚拟机名称,在此以复制 Wordpress 虚拟机为例。在弹出的右键菜单中选择“启用复制”命令。

在打开的“启用复制向导”对话框中,单击“下一步”按钮,进入到添加“副本服务器”界面,在该界面中输入副本服务器名称,随后单击“下一步”按钮。

系统对目标服务器进行验证,验证成功后打开“链接参数设置”窗口。

首先在该界面中设置好副本服务器的端口,在下面的身份验证类型中点选“使用 Kerberos 身份验证”类型。为了节省复制时间,建议勾选下面的“压缩通过网络传输的数据”复选框,设置后单击“下一步”按钮,进入到“选择复制 VHD”界面,这里系统列出指定虚拟机所对应的 VHD 文件,在此不建议修改。

单击“下一步”按钮,打开“配置恢复历史记录”界面,在此可以配置副本服务器存储主服务器点的数量(见图 4)。

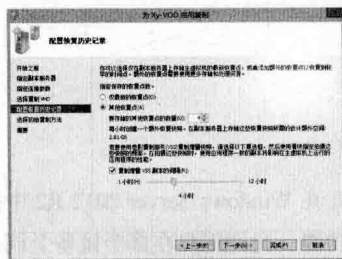


图 4 配置恢复历史记录

默认情况下,副本之间的复制周期为5分钟,也就是说,副本与原始虚拟机之间的差异是5分钟。这样我们可以选择多个恢复点,非常方便日后对逻辑故障或逻辑操作故障进行恢复。在建议选择“其他恢复点”的下面,“要存储的其他恢复点数量”中默认恢复点为4,我们可以根据自己的实际需要进行设置。随后,单击“下一步”,进入到“选择初始复制方法”界面,在此建议选择默认的“通过网络发送初始副本”选项。

随后,单击“完成”按钮退出设置向导对话框,此时Hyper-V主服务器开始向副本服务器复制文件。在Hyper-V管理器列表中,通过“任务状态”可以查看到当前数据复制进度。

虚拟机复制需要的时间取决于虚拟机本身数据的大小。通过上面的操作,我们将虚拟主服务器上的虚拟机复制到副本服务器中了。

之后,在“虚拟机管理器”界面,右键单击“Hyper-V管理器”名称,在弹出的右键菜单中选择“连接到服务器”命令,打开服务器连接列表。

點選“另一台计算机”,并在此输入副本虚拟机的名称,随后单击“连接”按钮,即可将副本服务器添加到该列表中。

切换到副本虚拟机服务器下,在“虚拟机”列表中,可以看到和主服务器上有一个名称完全相同的虚拟机,这就是主服务器上的虚拟机在副本服务器上创建的一个副本,该虚拟机状态为关机状态。

切换到主服务器列表,右键单击“wordpress”虚拟机,在弹出的右键菜单中单击“复制→查看复制运行状况”命令,打开当前虚拟机复制的运行状况界面,在此可以了解虚拟机的复制状态,以及两个副本之间的差异。

启用计划转移

虚拟机的两个副本完成后,下面就可以启用计划故障转移功能了。所谓计划的故障转移,就是将主服务器上的wordpress虚拟机在运行状态无数据损失的情况下,转移到副本服务器的wordpress虚拟机上运行。

操作时,首先将主服务器上“wordpress”虚拟机关机,右键单击该虚拟机名称,在右键菜单中选择“复制→计划的故障转移”命令,打开“计划的故障转移”对话框(见图5)。

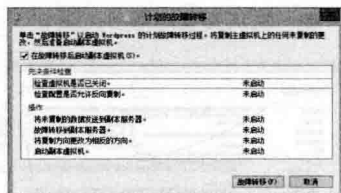


图5 计划的故障转移

在该界面中勾选“在故障转移后启动副本虚拟机”复选框,随后单击“故障转移”按钮,进入到“计划的故障转移”界面。

启动故障转移功能,在这个操作过程中,虚拟机会将主虚拟机上的最新数据复制到副本服务器上,随后在将副本服务器虚拟机会自动启动。

通过计划的故障转移功能,以后复制主机一旦意外宕机时,我们便可以在复制主机上执行“故障转移”,确保虚拟机系统的正常运行。

通过上面的操作,我们非常方便地将主服务器上的虚拟系统快速转移到副本服务器上,并且可以通过故障转移功能,随时将虚拟机中更新的数据及时进行备份及反向恢复。

Windows 7 中使用工作文件夹

河北 王春海

Microsoft 在 Windows Server 2012 R2 中推出了“工作文件夹”功能,允许用户在多个设备上同步“工作文件夹”目录中的数据。用户可以同步笔记本电脑和平板

电脑上的文件夹并编辑里面的文件,而此时文件夹处于离线状态,当用户下次连接上网络后,这些改变会进行同步。

应用需求

在最初的时候,工作文件夹的客户端只能是 Windows 8.1,当时笔者写了一篇文章“让工作文件夹与 BYOD 同步”的专题文章,详见 2014 年《网络运维与管理》。

后来 Microsoft 发布了用于 Windows 7 的“工作文件夹”版本,其 32 位下载地址为 <https://www.microsoft.com/zh-CN/download/details.aspx?id=42559>,64 位下载地址为 <http://www.microsoft.com/zh-CN/download/details.aspx?id=42558>。

笔者家中的计算机使用的是 Windows 10 系统,单位计算机使用的是 Windows 7 系统。由于家庭宽带早已升级到了 50M 的光纤,感觉到平常在单位、家里回来拷贝文件,使用 U 盘比较慢,使用 OneDrive,又感觉到速度比较慢,毕竟 OneDrive 是采用 Microsoft 的服务器。而单位有测试用的服务器,Active Directory、文件服务器这些都有,原来配置的用于“工作文件夹”的环境也有,就准备使用“工作文件夹”,在单位与家中的 PC 间同步数据。

家里的计算机,Windows 10,信任并下载根证书,配置工作文件夹很方便,这些不一一介绍。

同步设置

现在的问题是,单位计算机安装的是 Windows 7 企业版,升级到 SP1。在安装了用于 Windows 7 的“工作文件夹”软件之后,提示需要加入到域才能工作。而加入到域之后,打开“控制面板→工作文件夹”后,出现如图 1 所示的错误。主要错误信息是“工作已停止。已被安全策略阻止”,更具体一些是“由于服务器使用的是 Windows 7 不支持的密码策略,工作文件夹不能同步到这台电脑。”



图 1 同步已停止

刚开始以为是当前计算机的密码策略与服务器的密码策略不同。在 Windows 7 这台计算机上执行 Secpol.msc,打开“安全设置→账户策略→密码策略”,发现与服务器的密码策略相同。

因为工作文件夹采用的是 <https://mh09.heinfo.edu.cn> 的站点,之后我又将该站点添加到 IE 浏览器的“本地 Intranet”区域。问题仍然没有解决。

之后查看 Microsoft 的帮助文档,使用 PowerShell 命令,解决。切换到提供“工作文件夹”Windows Server 2012 R2 的服务器中,运行 PowerShell,执行以下命令:

Set-SyncShare fs-home -PasswordAutolock ExcludeDomain “heinfo.edu.cn”(如图 2 所示)。



图 2 执行 PowerShell

其中 fs-home 是工作文件夹的共享目录。而 heinfo.edu.cn 是笔者的域名。

执行之后,返回到 Windows 7 的计算机中,在“服务”中先停止“Work Folders”(如图 3 所示)。

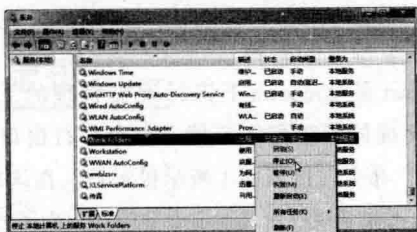


图 3 停止工作文件夹服务

之后打开“控制面板→工作文件夹”,状态为“正在同步”。

在同步完成之后,状态正常。单击“打开文件位置”按钮,打开工作文件夹。至此问题解决。

批处理统计信息

广州 张鹏 湛得志

设计思路

为了满足信息采集需求，批处理程序需要具备采集和传输两方面的功能。信息采集使用系统自带的命令行工具，如 ipconfig、diskpart 等命令实现。采集的信息使用 FTP 进行传输，利用网络中的 FTP 服务器接收各终端上传的结果。

常用命令及实现

下面对信息采集中较为重要的几个命令进行简要介绍。

1. 硬盘信息的采集

diskpart 是 Windows 下进行硬盘管理的工具，它是一个集成的管理配置环境。在命令行窗口中输入“diskpart”命令，进入图 1 所示提示符。在该环境下，可使用若干命令对硬盘进行查看和管理。为了方便批处理程序执行，该工具也支持脚本文件方式执行，采用“diskpart /s 脚本文件”的方式执行。其中“脚本文件”为 diskpart 集成环境的命令集合。由于只需要查看硬盘信息，这里用的 diskpart 命令只包括 list、select 和 detail 三个命令。

```
Microsoft DiskPart 版本 6.1.7601
Copyright (C) 1999-2008 Microsoft Corporation.
在计算机上: PC-201510141531
DISKPART>
```

图 1 diskpart 命令提示

2. 系统信息的采集

获取操作系统信息可以有多种方法，其中 Systeminfo 命令获取的信息十分丰富，包括操作系统名称、版本、系统型号、处理器及补丁等若干信息，是较为理想的信息采集手段。

但是在实际使用过程中，systeminfo 命令无法正常将扫描的信息存入记录文件中。估计这可能与 systeminfo 命令的运行方式有关系。由于需要统计信息

没有那么详细，于是便采用“wmic os get name”同样可以获得操作系统类型，再使用“ver”获取操作系统的详细版本号。

3. 网络信息的采集

网络信息采用 ipconfig /all 可以获取，该命令在日常网络配置管理中经常使用，此处不再进行详细介绍。

4. 采集信息的上传

采集信息文件通过 FTP 工具上传到网络中的 FTP 服务器中去。为了方便批处理执行，FTP 工具采用脚本方式执行，其格式为“ftp -s:filename”。其中 filename 为含有若干 FTP 命令集合的脚本。

批处理脚本

写好的脚本如下所示。

```
set /p input= 计算机使用人 :
echo off
hostname >%input%.txt
@echo 开始构造 DISKPART 脚本
echo list disk >t.txt
echo select disk 0 >>t.txt
echo detail disk >>t.txt
echo exit >>t.txt
diskpart /s t.txt >>%input%.txt
@echo 开始获取网络配置
ipconfig /all>>%input%.txt
@echo 开始获取操作系统信息
wmic os get caption>>%input%.txt
ver>>%input%.txt
@echo 开始构造 FTP 的脚本
echo open [ip address]>ftp.tmp
echo [username]>>ftp.tmp
echo [password]>>ftp.tmp
echo dir>>ftp.tmp
```

```
echo cd /upload/temp>>ftp.tmp
echo put %input%.txt>>ftp.tmp
echo bye>>ftp.tmp
@echo 开始上传
ftp -i -s:ftp.tmp
@echo 删除生成文件
del ftp.tmp
del t.txt
del %input%.txt
pause
```

运行后，输出结果如图 2 所示，可以考到生成的脚本已经被上传到 FTP 服务器的文件目录之中。

```
C:\Users\Administrator\Desktop\临时>echo off
开始构造DIEXPLOIT 脚本
开始构造攻击配置
开始构造操作系统信息
开始上传信息文件
ftp> open 18.181.1.43
连接到 18.181.1.43.
228 Serv-U FTP Server v6.4 for WinSock ready...
用户(18.181.1.43:(none)):
230 User logged in, proceed.
ftp> ECHO 处于关闭状态。
无响应。
ftp> dir
200 PORT Command successful.
150 Opening ASCII mode data connection for /bin/ls.
drwxr-xr-x 1 user group 0 Mar 13 2012 .
drwxr-xr-x 1 user group 0 Mar 13 2012 ..
drwxr-xr-x 1 user group 0 Oct 12 2013 data
drwxr-xr-x 1 user group 0 Nov 13 2013 document
drwxr-xr-x 1 user group 0 Dec 22 20120 software
drwxr-xr-x 1 user group 0 Jun 5 2013 upload
226 Transfer complete.
ftp> 收到 371 字节, 用时 0.00秒 371000.00千字节/秒。
ftp> cd /upload/ghp
250 Directory changed to /upload/ghp
ftp> put test.txt
200 PORT Command successful.
150 Opening ASCII mode data connection for test.txt.
226 Transfer complete.
ftp> 发送 5798 字节, 用时 0.15秒 38.47千字节/秒。
ftp> bye
221 Goodbye!
删除生成文件
请停止继续连接...
```

图 2 统计结果上传

经验总结

批处理程序是个十分强大的工具集，可以实现丰富了管理功能。采用批处理程序进行计算机信息采集，可以降低终端用户采集信息的难度，降低网管人员的工作量。

删除孤立的虚拟机

在使用 VMware View 桌面的过程中，如果由于多种原因（例如重新安装了 vCenter Server）导致 View 桌面池丢失，想要在 View Administrator 中删除这些孤立的虚拟机与桌面池，可以使用如下的方法。

登录 View Composer 删除孤立的虚拟机

进入 View Composer 的服务器，打开 View Composer 安装位置，复制该路径（如图 1 所示。默认情况下，此路径为 C:\Promram Files (x86)\VMware\VMware View Composer。



图 1 复制路径

打开“系统属性→环境变量→系统变量”，将该路径添加到 Path 路径最后。说明，在原来的路径后面添加一个英文的分号（；），再粘贴此路径。

之后进入提示符，使用 sviconfig 命令，删除 View Administrator 中孤立的虚拟机，在此需要删除的虚拟机名称是 win7x-001、win7x-002 等虚拟机，每条命令删除一个虚拟机。命令如下：

```
sviconfig -operation=removesviclone
```

-VmName=win7x-001

Enter View Composer admin password:*****

Get clone ID.

Remove linked clone.

RemoveSviClone operation completed successfully.

其中，在删除虚拟机的时候，需要输入 View Composer 的管理员密码（如图 2 所示）。

```
C:\>vsiconfig -operation=removeSviClone -VmName=win7x-001
Enter View Composer admin password:*****
Get clone ID.
Remove linked clone.
RemoveSviClone operation completed successfully.
```

图 2 删除孤立的虚拟机

之后依次使用命令，删除这些孤立的虚拟机。

登录 View 连接服务器删除数据库

之后登录 View 连接服务器，使用 adsiedit.msc，删除虚拟机池。

1. 以管理员的身份登录到 Horizon View 连接服务器，打开“运行”对话框，输入 adsiedit.msc，然后回车键。

2. 打开“ADSI 编辑器”之后，右击 ADSI 编辑器，在弹出的对话框中选择“连接到”（如图 3 所示）。



图 3 连接到

3. 在弹出的“连接设置”对话框中，在“连接点”处单击“选择或键入可分辨名称或命名上下文”，并在栏目中输入 DC=vdi，DC 搜索=vmware，DC=int（英文输入，此名称与你的 Active Directory 域名无关），在“计算机”处单击“选择或键入域或服务器”，输入 localhost:389，或者输入你的计算机名称及端口号，例如本示例中为 vcs.heuet.com:389，之后单击“确定”按钮。

4. 返回到 ADSI 编辑器，依次展开 OU=Server Groups，然后删除孤立的虚拟机桌面池，在此为 CN=Win7x。

5. 之后展开 OU=Applications，删除 CN=Win7x。

再次登录 View Administrator，可以看到孤立的虚拟机桌面池已经被删除（如图 4 所示）。

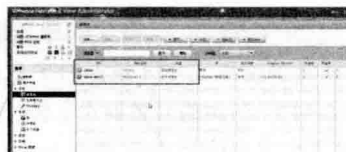


图 4 桌面池已经被删除

在“资源→计算机”中可以看到，孤立的虚拟机已经被删除。

❖ 修改 Manifest 控制权限

广州 何文韬

在 Windows 7 环境下，当使用普通用户账号运行某些应用程序（程序图标显示有盾牌）的时候，系统会弹出对话框，要求输入管理员账号和密码，否则无法运行。也就是说，这类应用程序只允许管理员运行，普通用户则完全无法运行。

但同一应用程序在 Windows XP 环境下却能基本运行，只是部分功能因没有管理员权限而无法使用。为安全起见，公司电脑一般都不会赋予用户账号管理员权限，

这样一来，很多程序都会无法在 Windows 7 下运行，会造成相当的不便。这是由于 Windows 的 UAC（用户账户控制）安全机制导致的。

用户账户控制机制

Windows 从 Vista 开始引入用户账户控制机制，当应用程序需要进行一些操作系统层面，或者影响其他用

户操作的设置,比如更改控制面板设置、删除系统文件、修改注册表等,操作系统便会弹出对话框,提示用户输入管理员账号密码,获得许可后方可继续。

UAC的这种临时提升用户权限的设计,大大提高了Windows的安全性,应用程序的一些操作必须要获取到管理员用户的许可方能运行,这样可以防止恶意软件和间谍软件在未经许可的情况下,在计算机上运行安装或者对计算机进行更改。

凡是图标显示有盾牌的可执行文件,都需要管理员权限才能完全正常地运行,但也有可能该应用程序只是部分功能需要管理员权限而已。很多情况下,我们只需用应用程序的一般功能,所以我们需要强制可执行文件以普通用户权限运行。

默认情况下,可执行文件 EXE 是以当前用户权限运行的,那么操作系统是如何知道应用程序需要使用管理员权限运行而弹出对话框提示用户呢?

操作系统是通过读取 Manifest 清单文件来获取 EXE 文件运行所需的权限。Manifest 清单文件是一个后缀为 .manifest 的 XML 文件,保存了应用程序的配置元数据。该 Manifest 可作为文件存储在应用程序相同的目录下,也可作为一种资源嵌入在可执行文件内部。

修改 Manifest 文件

我们可以通过修改 Manifest 文件,来控制应用程序的运行权限。以下分为外置和内置两种清单文件的修改方法。

1. 外置同名 Manifest 文件

以软件“一号店在线客服”为例,软件安装后,修改程序目录(C:\Program Files(x86)\yhd)的文件夹权限,编辑 Users 用户组,添加“修改和写入”权限。在“高级”菜单中,勾选“更改权限→使用可从此对象继承的权限替代所有子对象项目”。然后以普通用户账号登录,运行主程序(im-desktop.exe),系统弹出 UAC 对话框。

用记事本编辑跟程序位于同一目录的 im-desktop.exe.manifest 文件(见图1)

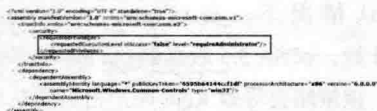


图1 编辑 im-desktop.exe.manifest 文件

配置中有一个 requestedExecutionLevel 项,这个项

用于配置当前应用请求的执行权限级别。这个项有3个值可供选择:

asInvoker: 应用程序就是以当前的权限运行。
highestAvailable: 应用程序以当前用户可以获得的最高权限运行。
requireAdministrator: 应用程序仅以系统管理员权限运行。

所以,我们只需要将 requestedExecutionLevel 项目设置为 asInvoker 或者 highestAvailable, 程序就能以当前用户账号正常运行了。其中, highestAvailable 和 requireAdministrator 这两个选项都可以提示用户获取系统管理员权限。

两个选项的区别在哪里呢?它们的区别在于,如果我们不是以管理员账户登录,而应用程序设置为 requireAdministrator, 那么应用程序就直接运行失败,无法启动,也就是强制程序以管理员账号运行。而如果设置为 highestAvailable, 则应用程序可以运行成功,只是以当前账号的最高权限运行而不是系统管理员权限运行。另外,直接将该 Manifest 文件删除也可以强制操作系统以当前用户运行。

2. 可执行文件内置 Manifest 文件

以软件“美图秀秀”为例,安装软件后,使用普通账号运行会弹出 UAC 对话框,

因其 Manifest 清单文件内置在 EXE 文件里,无法直接编辑。

(1) 首先下载并安装可执行文件编辑软件 Resource Hacker (<http://www.angusj.com/resourcehacker/>)。

(2) 接着,用管理员账号运行 Resource Hacker 软件(鼠标右键主程序以管理员身份运行),然后点击“File→Open”,选择美图秀秀的主程序 Xiuxiu.exe,点击左侧的资源列表中的 Manifest→1:1033(见图2)。这时候就看到了内置在 EXE 文件中的清单文件内容了,该文件内容和需要修改的内容都跟之前外置的清单文件一样,只要将 requestedExecutionLevel 项目修改为 asInvoker 或者 highestAvailable 即可。



图2 点击左侧的 Manifest→1:1033

(3) 修改后,点击工具栏中的 Compile Script,接着点击 Save,程序会自动备份原文件为 XiuXiu_original.exe。

(4) 注销并重新登录一下当前的普通用户，运行 xiuxiu.exe，程序就可以顺利运行了。

注意事项

现在，越来越多的应用程序运行时需要提升权限到管理员级别，这样可以提高软件的使用体验。但是，企业办公电脑由于安全性和管理的需要，一般不允许赋予普通用户本机管理员的权限，这样一来，很多软件都无

法使用。通过关闭 UAC 功能或者修改 Manifest 清单文件，都可以令普通用户能基本运行这类应用程序。不过，关闭 UAC 后，即与 Windows XP 环境软件的运行机制类似，只能通过鼠标右键选择“运行”来提升运行权限，而且基于安全性的考虑，不建议关闭 UAC 功能。

需要注意的是，修改清单文件后，不能保证软件可以百分百正常运行，修改后有时需要注销再登录当前用户或者重启系统才会生成。还有，清单文件修改前要注意对 EXE 文件和 Manifest 文件原文件做好备份。

部署 vCenter Server 经验

河北 王春海

部署 vCenter Server Appliance 时的“客户端集成插件”问题

从 vCenter Server Appliance 6.0 开始，VMware 改变了部署 vCenter Server Appliance 的方式，vSphere 不再支持使用 vSphere Client 或 vSphere Web Client 部署 vCenter Server Appliance，需要安装“客户端集成插件”并执行光盘中的 vcsa-setup.html，以 HTML 的方式部署。

虽然在 vCenter Server Appliance 光盘镜像中，客户端集成插件的名称都是 VMware-ClientIntegration Plugin-6.0.0.exe，但不同版本 vCenter Server Appliance 安装光盘中的“客户端集成插件”的文件大小是有区别的，如图 1 所示，这是三个不同版本的客户端集成插件的安装文件的修改日期及大小。

名称	修改日期	大小
VMware-ClientIntegrationPlugin-6.0.0-2562643.exe	2015/3/5 1:54	97,312 KB
VMware-ClientIntegrationPlugin-6.0.0-3040690.exe	2015/9/4 8:06	97,362 KB
VMware-ClientIntegrationPlugin-6.0.0-3343019.exe	2015/12/17 11:57	97,270 KB

图 1 不同版本的客户端集成插件的大小

你可以查看该安装程序的“数字签名”来对比，这些客户端集成插件有不同的签名日期。

所以，在部署 vCenter Server Appliance 6.x 的时候，需要安装对应版本 vCenter Server Appliance 光盘镜像中的“客户端集成插件”，不能使用以前版本的客户端集成插件，当安装的客户端集成插件与所部署 vCenter

Server Appliance 版本不一致时，会出现如图 2 所示的提示，并且不会显示错误的原因。



图 2 部署时不能继续

如果出现图 2 的错误，请在“控制面板→程序和功能”中，卸载安装的“VMware Client Integration Plug-in 6.0.0 (客户端集成插件)”。

最后，在 vCenter Server Appliance 安装光盘的 vcsa 目录中，执行“VMware Client Integration Plug-in 6.0.0.exe”安装程序，重新安装客户端集成插件，再次启动安装向导进行部署即可。

更改 vCenter SSO 的密码策略

在默认情况下，自 vCenter Server Appliance 5.5 Update 1 开始，vCSA 5.5 版强制执行本地账户 (Root) 密码策略，该策略会导致 Root 账户密码会在 90 天后过期。当密码到期后，会将 Root 账户锁定。关于这一问题，VMware 在 KB2099752 中有过介绍，详细链接可见：

<https://kb.vmware.com/selfservice/microsites/>

search.do?language=en_US&cmd=displayKC&externalId=2099752。

但是，如果你使用 Windows 的 vCenter Server，在使用默认的 administrator@vsphere.local 登录 vSphere Web Client 的时候，如果你的安装已经接近 90 天，则有可能会发出提示“您的密码将在 X 天后过期”。无论是预置的 Linux 版本的 vCenter Server (VCSA)，还是安装在 Windows Server 上的 vCenter Server，都会有这个提示。

对于“您的密钥将在 X 天后过期”的提示，是 vCenter Server 的 SSO 的密码策略的生命周期设置为 90 天的原因，vSphere 管理员可以通过修改密码策略，去掉这一提示，并设置密码永不过期。

1. 使用 IE 浏览器登录到 vSphere Web Client，在导航器中单击“系统管理”，在“系统管理→Single Sign-On→配置”中，单击“策略→密码策略”选项卡，然后点击“编辑”按钮（如图 3 所示，在此可以看到“最长生命周期”为“密码必须每 90 天更改一次”。

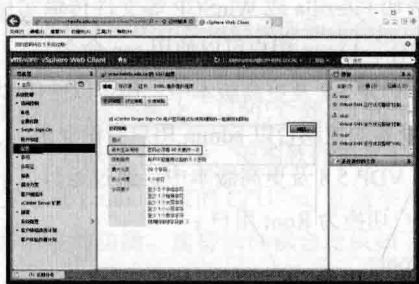


图 3 密码策略

2. 在“编辑密码策略”对话框，将“最长生命周期”修改为 0 天，表示“密码永不过期”，然后单击“确定”按钮。在“密码格式要求”选项中，还可以修改密码的最大长度、最小长度、字符要求等条件，这些要求比较简单，每个管理员都能理解其字面意思，在此不再介绍。

3. 设置完成之后，返回到“策略→密码策略”页，在“最长生命周期”中可以看到，当前策略为“密码永不过期”（如图 4 所示）。

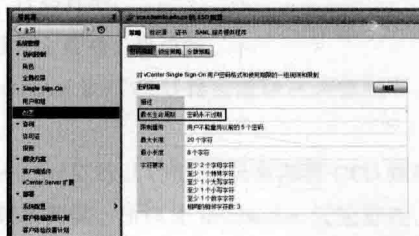


图 4 密码永不过期

vCenter 升级问题

在升级 vCenter Server 的时候，最好将 vCenter Server 的安装光盘镜像上传到与 vCenter Server 所在主机的本地存储或本地主机能访问的共享存储，不能使用 vSphere Client 连接到 vCenter Server，再加载 vSphere Client 的光盘镜像的方式升级 vCenter Server。因为在升级 vCenter Server 的过程中，vCenter Server 会有一段时间停止服务，如果是加载 vSphere Client 客户端镜像的方式升级，在 vCenter Server 停止服务的过期中，加载的 vSphere Client 镜像会断开连接，从而导致升级失败。

vSphere Web Client 英文界面问题

vSphere Web Client 支持中文、英文、日文等多语言并自适应浏览器客户端。但在某些时候，vSphere Web Client 侦测失败时会显示英文。例如，在中文的 Windows 10 中，使用 Chrome 浏览器时，显示为英文界面。

其实，和 Client 端修改的方法差不多，只需要在我们的登录地址后面加入一个参数 /? locale=en_US 或者 /? locale=zh_CN 即可。例如：https://hostname:9443/vsphere-client/?locale=en_US，即可将本来是中文的登录界面改为英文。

显示 ESXi 的正常运行时间为 0 秒

在启动 ESXi 中的虚拟机时，如果出现“没有与虚拟机兼容的主机”，并且检查，发现当前群集中每个主机的“正常运行时间”为“0 秒”，并且 CPU 与内存显示“已用”为 0 时，重新启动群集中的每个主机即可。

1. 某 vSphere 数据中心，尝试打开一个虚拟机电源。
2. 弹出“打开电源故障”对话框（如图 5 所示）。



图 5 打开电源故障

3. 依次查看当前群集中的每个主机，在“摘要”中，看到主机“正常运行时间”为 0 秒，并且 CPU 的已用频率为 0.00 Hz，内存已用为 0.00B。

4. 如果使用 vSphere Client 查看主机摘要，则显示

同样的情况（如图 6 所示）。



图 6 主机已用资源为 0

5. 对于这种情况，请重新启动 ESXi 主机即可。如果群集中有多台主机，请依次启动，不要同时启动。例如，右击 172.18.96.43，选择“重新引导”。

6. 等主机引导成功之后，在“摘要→资源”选项中，可以看到内存与 CPU 使用情况（如图 7 所示）。然后，将其他主机依次启动即可。



图 7 资源使用显示正常

在 IE11 不能初始配置 VDP 5.5.x 及 VDP 6.0 的问题

VMware vSphere Data Protection (VDP) 是 VMware 虚拟机备份软件。在部署 VDP 5.x 或 6.0 的时候，如果出现“无法显示此页”（如图 8 所示）。



图 8 无法显示此页

出现该问题的原因是 Firefox、Chrome 和 Internet Explorer 取消了对 DSA 密码的支持，而 VMware vSphere Data Protection 5.x 和 6.0 使用 DSA 密码与浏览器通信。Firefox 发行版本 37 同 Chrome 发行版本 40.0.2215.115m 一样移除了 DSA 密码。

这个问题在 VMware vSphere Data Protection (VDP) 6.0.1 中已得到解决。如果你要在 VDP 6.0 或更低版本中解决此问题，请在 VDP 设备中运行附加的 2111900_VDPHotfix.SHA2.sh.zip 文件。

但是，不要在安装和配置 VDP 之前运行该脚本，否则，向 vCenter 注册 VDP 将失败。所以，在安装 VDP 并在第一次运行时，使用 IE8 配置 VDP（管理员可在 VMware 虚拟机中，安装 Windows 7 并不升级到 IE10 或 IE11 即可），运行 VDP 初始配置向导。

要在 VDP 设备中运行附加的 2111900_VDPHotfix.SHA2.sh.zip 文件，请执行以下操作：

1. 将 2111900_VDPHotfix.SHA2.sh.zip 文件复制到 VDP 设备，并将其放置在 /tmp 目录中。Windows 用户应使用诸如 Filezilla 或 WinSCP 等文件传输实用程序来执行此操作。Linux 用户可以使用 scp 命令。

2. 在 VDP 5.8 及更高版本中，您可以使用 SSH 会话或 VDP 设备的控制台以 admin 用户身份登录。

3. 在 VDP 5.8 及更高版本中，通过运行以下命令从 admin 用户切换为 Root 用户：

```
su - root
```

4. 通过运行以下命令将目录更改为 /tmp：

```
cd /tmp
```

5. 运行以下命令：

```
a.unzip 2111900_VDPHotfix.SHA2.sh.zip
```

```
b.CD into folder 2111900_VDPHotfix.SHA2.sh
```

```
c.chmod a+x VDPHotfix_SHA2.sh
```

```
d./VDPHotfix_SHA2.sh
```

此热修补程序会删除 VDP tomcat 服务的旧 SHA1 证书，并生成新的 SHA2 证书。



调整 Linux 系统 CPU 频率

▼ 西安 解宝琦 薛民华

现在电脑 CPU 耗电很大，按需调节 CPU 频率对普通桌面及移动设备节能有重要的意义。目前，多数 Linux 发行版都已经默认启用了这个功能，但在一些像数据库、集群系统等特别需要 CPU 高性能的服务器环境中，Linux 提供的这种对 CPU 频率调节的功能对 CPU 性能使用受到一些限制，不利于系统性能的更好发挥。为此，需要 Linux 系统管理员对相关参数优化及设置来确保 CPU 性能最大化。

本文将针对应用中常见的 RedHat 6、7 系列及 Debian Gnu/Linux 8 系列中 CPU 频率调整工具的使用进行描述，以方便 Linux 用户进行该方面工作的优化。

在 Linux 中，内核的开发者定义了一套框架模型来完成 CPU 频率动态调整这一目的，它就是 CPUFreq 系统。尽管在各个 Linux 发行版中，前端软件稍有差异，但其最终都会通过 Linux 内核的 CPUFreq 系统来实现 CPU 频率动态调整的功能。这些软件都会提供如下 CPU 模式（governor 参数）：

1.ondemand

系统默认的超频模式，按需调节，内核提供的功能，不是很强大，但有效实现了动态频率调节，平时以低速方式运行，当系统负载提高时自动提高频率。以这种模式运行不会因为降频造成性能降低，同时也能节约电能和降低温度。一般官方内核默认的方式都是 ondemand。

流畅度：一般，流畅。

2.interactive

交互模式，直接上最高频率，然后看 CPU 负荷慢慢降低，比较耗电。

流畅度：最高，极流畅。

Interactive 是以 CPU 排程数量而调整频率，从而实现省电。

InteractiveX 是以 CPU 负载来调整 CPU 频率，不会过度把频率调低。所以比 Interactive 反应好些，但是省电的效果一般

3.conservative

保守模式，类似于 ondemand，但调整相对较缓，想省电就用他吧。Google 官方内核，kang 内核默认模式。

流畅度：高，流畅。

4.smartass

聪明模式，是 I 和 C 模式的升级，该模式在比 interactive 模式不差的响应前提下，会做到了更加省电。

流畅度：最高，流畅。

5.performance

性能模式，只有最高频率，从来不考虑消耗的电量，性能没的说，但是耗电量……

流畅度：流畅度高于 interactive。

6.powersave

省电模式，通常以最低频率运行。

流畅度：极低。

7.userspace

用户自定义模式，系统将变频策略的决策权交给了用户态应用程序，并提供了相应的接口供用户态应用程序调节 CPU 运行频率使用。也就是长期以来都在用的那个模式。可以通过手动编辑配置文件进行配置。

流畅度：根据设置而定。

8.Hotplug

类似于 ondemand，但是 CPU 会在关屏下尝试关掉一个 CPU，并且带有 deep sleep，比较省电。

流畅度：一般，流畅。

在进行 CPU 频率优化之前，我们首先需要使用命令 `lsmod | grep "acpi_cpufreq"` 查看内核是否加载了 acpi_cpufreq 模块，如果加载了此模块，按照一般情况发行版都会将 CPU 设置为“ondemand”模式。

之后，可以通过命令 `cat /sys/devices/system/cpu/cpu0/cpufreq/scaling_available_frequencies` 进一步确认 CPU 节能模式，但此时用户无法进行修改，需要进行修改必须使用命令安装 cpufreq 管理软件。在 Debian

Gnu/Linux 下使用如下命令：apt-get install cpufrequtils，在 RedHat6 一下版本中使用如下命令：yum install cpuspeed，在 RedHat7 系列版本中使用如下命令：yum install kernel-tools。之后我们就可以通过修改相应系统所在配置文件并重启相关服务，使 CPU 按照我们的要求配置参数进行运行。

Debian Gnu/Linux 8、RedHat6 一下版本、RedHat7 系列版本 cpufreq 管理软件配置文件分别为 /etc/init.d/cpufrequtils、/etc/sysconfig/cpuspeed、/setc/sysconfig/cpupower。修改 Debian Gnu/Linux 8 配置文件中 GOVERNOR="ondemand" 为 GOVERNOR="performance"，RedHat6 一下版本配置文件中 GOVERNOR 为 GOVERNOR=performance，RedHat7 系列版本配置文件中 CPUPOWER_STOP_OPTS="frequency-set -g ondemand" 为 CPUPOWER_

STOP_OPTS="frequency-set -g performance"。

在 Debian Gnu/Linux 8、RedHat6 一下版本、RedHat7 系列版本中分别执行 /etc/init.d/cpufrequtils restart、/etc/init.d/cpuspeed restart、systemctl restart cpupower.service 命令即可重启相关 cpufreq 管理软件。

从 kernel 3.9 开始，名为 pstate 的新的功率驱动程序将会在以下的驱动程序之前自动为现代的 Intel CPU 启用。该驱动会优先于其他的驱动程序，因为它是内置驱动，而不是作为一个模块来加载。该驱动自动作用于 Sandy Bridge 和 Ivy Bridge 这两个类型的 CPU，在该模式下，CPU 只能被设置成 performance 或者 powersave 模式。如果您在使用这个驱动的时候遇到问题，建议您在 Grub 的内核参数中对其禁用（即修改 /etc/default/grub 文件，在 GRUB_CMDLINE_LINUX_DEFAULT=后添加 intel_pstate=disable）。

用 VHD 打造双系统

广西 周瑜

Windows 7 和 Windows XP 双系统，有的人选择用常规安装方法在本地磁盘分别安装这两个操作系统，但这样不仅需要划分一个不小于 10GB 的主分区，还需要修改系统启动菜单，相对复杂且容易出问题。有的人选择使用 VMware 等软件制作虚拟机的方法实现，但会占用大量硬件资源。其实，使用 Windows 7 支持的 VHD 也可实现 Windows 7 和 Windows XP 双系统环境，而且这种方法技术难度相对较低，硬件资源占用较少。

VHD 是 Microsoft Virtual Hard Disk format（微软虚拟硬盘文件）的简称，使用 VHD 技术，可以将一个后缀名为“.vhd”的文件虚拟成一个硬盘来使用，该虚拟盘如同真实的硬盘一样，可以对其进行任何操作，包括格式化、分区、加载、删除等。在 VHD 虚拟盘中，不仅可以存储数据、安装软件，还可以在“灌装”独立的系统，来打造多系统使用环境，而且系统迁移方便。

在此，介绍利用 Windows XP VHD 辅助处理工具 2011（该工具是基于 VBOOT 开发，用于创建 VHD，

支持把 Ghost 版 Windows XP 或者安装版的 ISO 镜像文件装入 VHD 的辅助处理工具）在 Windows 7 系统下安装 Windows XP 系统的方法。

1. 关闭 Windows 7 系统的 UAC（用户账户控制）

打开控制面板，再选择用户账户和家庭安全，在用户账户中，更改用户账户设置为最低权限线，即“从不通知”即可。

2. 配置 Windows XP VHD 辅助处理工具

在 Windows 7 系统中启动该工具后，选择创建 VHD、VHD 的位置、大小，以及动态扩展还是固定大小，再选择需要安装 Windows XP 系统的 Ghost 文件或者 ISO 镜像文件。在此用快捷方便的 Ghost 文件，确定后会启动 Ghost 软件，将 Ghost 文件解压至创建好的 VHD 磁盘内。解压完成后，软件会提示是否将 Vboot 导入硬盘和注册表，此处一定要选择“是”，将导入 vboot 文件夹、vbootldr、vbootldr.mbr 两个文件以及

相应的注册表，否则无法选择操作系统。

3. 搞定 Vboot

在软件的第一个界面，选择“挂载/卸载 VHD”，选择新建的 XP 系统 VHD 文件，再点击挂载，即可打开安装 XP 的 VHD 磁盘，在 Windows XP 系统分区/Windows/system32/drivers，找到 vbootdisk.sys，可以用 Ultraedit 软件打开文件，搜索“76220503a426f3”字串，

把其中的 76 改为 eb。此处推荐使用已经修改好的文件，不仅简单而且也不容易出错。

4. 完成 Windows XP 系统安装

重启操作系统，会出现一个双系统（Windows 7 和 Windows XP VHD）选择界面，选择 Windows XP VHD，系统会自动完成 Ghost 系统安装。

❖ 将 Hyper-V 安装到 Windows 10

威海 赵永华

Hyper-V 安装条件

在 Windows 10 中安装 Hyper-V 具有这样一些前提条件：

1.OS 版本：只有在 Windows 10 Enterprise Editions 或 Pro 版本才能安装 Hyper-V。

2.CPU 架构：Hyper-V 仅能运行于 64 位系统，而且要求 CPU 支持 SLAT（Second Level Address Translation），在微软网站有一个免费工具 CoreInfo 可以了解当前系统 CPU 是否支持运行 Hyper-V（<https://technet.microsoft.com/en-us/sysinternals/cc835722>）。

3. 系统的 RAM 至少 4GB，这是因为 Hyper-V 有一项动态内存功能 DM（Dynamic Memory），能够对客户端 VMs 指定内存分配值区间（最小和最大值）。

SP1、Windows 8/8.1、Windows 10、Windows Server 2008 SP2/R2 SP1、Windows Server 2012/ 2012 R2；还可以是多个版本的 UNIX/Linux，包括 CentOS、Red Hat Enterprise Linux、Debian、SUSE、Oracle Linux、Ubuntu 以及 FreeBSD。

安装 Hyper-V 操作

现在我们就在 Windows 10 下开始安装 Hyper-V。

右键点击“开始”按钮，选择“Programs and Features”，然后选择“Turn Windows Features on or off”，点选“Hyper-V”之前勾选所有组件后点击 OK，重启即可。

这是 GUI 方式，还可以用 PowerShell 命令将 Hyper-V 安装到 Windows 10，具体命令如下所示：

```
Enable-Windows OptionalFeature -Online
-FeatureName Microsoft-Hyper-V -All
```

适用系统

在作为 Guest VMs 的 Windows 10 Hyper-V Host，可以运行多种操作系统，包括：Vista SP2、Windows 7/



值得关注的 ReFS

威海 赵永华

ReFS：可靠可扩展的磁盘结构

ReFS 将 B+ 树作为惟一且通用磁盘结构，借此展现磁盘的全部信息。ReFS 中所有元数据校验工作都可在树层面进行，这些校验值会独立于树页面本身，单独保存。这样可避免各种形式磁盘错误。

ReFS 能够实时检测和修复数据错误，无需卸载或干扰访问相应的卷。当一个文件被读取，读取文件的校验与存储的校验相比较，错误被自动检测。

在 ReFS 中，校验被放到文件元数据。一个附加的称为 Integrity Streams 的可选功能，确保更改写入时，它们被写入到一个不同的成员卷，以确保原始数据不受损害。这种错误检测对抗位损坏，磁盘上存储数据的降解，以及硬件故障、固件故障等破坏性事件，不影响联机文件系统的可用性。

ReFS 还包含了对文件内容进行校验的额外功能。通过启用名为 Integrity Streams 的选项，ReFS 会将文件改动写入到不同于原始位置的其他位置。使用了一种在写入事务中进行分配的模式（也叫做“写入时复制”）。这种方法可提供最大化的可靠性，同时无需采用日志结构的文件系统，既可避免在磁盘更新过程中，由于断电导致随机写入以及大量写入操作产生的问题。

为此，您可以通过自动化的方式将元数据的更新操作写入到其他位置，不对原数据进行原位更新。

ReFS 设计上可以充分满足 Windows 存储栈的各种指标，通过其他栈层提供最大化的灵活性与兼容性。兼容各种常用软件，如备份与反病毒应用程序，ReFS 在设计上依然能够很好地与存储栈的其他层完美配合。

ReFS 可无缝利用多台计算机以及虚拟磁盘上共享的存储池，并可在存储池之间实现无缝转换，在存储空间或 ReFS 基础之上提供额外的容错能力。

ReFS 的局限性

ReFS 继承了 NTFS 文件系统的出色功能，例如 BitLocker 驱动器加密、增强安全性的访问控制列表（ACL）、USN 日志、变更通知、重解析点、卷快照、SymLinks/Junctions/Mount points、文件 ID 以及 Oplocks。另外，ReFS 还可使用与客户端上任何操作系统访问 NTFS 卷时相同的文件访问 API 进行访问。

但是，ReFS 也有一些重要限制，包括：

1. 无法将原有 NTFS 磁盘区直接转换为 ReFS 格式，只能在两种文件系统间以手动方式搬移与复制资料。

2. ReFS 不能作为启动分区，这意味着 Server 2012 系统必须混合使用 NTFS 与 ReFS 两种文件系统，并以 NTFS 分区来启动。

3. ReFS 不适用于移动储存如移动硬盘和 USB 盘，ReFS 本身并未含有重复数据删除功能，也无法与 Server 2012 新增的重复数据删除功能并用（Server 2012 的重复数据删除功能，仅适用于 NTFS 文件系统磁盘区）。

4. ReFS 本身未内置可写入的快照功能，用户需通过其他工具软件，直接从 ReFS 底层的 Storage Space 虚拟磁盘建立可写入快照。

ReFS v2 有哪些改进

在 Windows 8 及 Windows Server 2012 中，我们已经见识到了 ReFS v1 这种新颖的磁盘系统，不过这种所谓可靠性文件系统，并没有让我们看到比常见的 NTFS 有多少优势，况且它主要针对的 Windows Hyper-V 磁盘。如今，ReFS v2 明显的技术改良让笔者顿时眼前一亮。

这里，笔者不禁想到了在 Windows 8/ Windows Server 2012 中出现的针对磁盘阵列的 Storage Spaces 技术，它提供了三种存储模式，即简约型（Simple）、镜像型（Mirror）和奇偶校验型（Parity）。Simple 模式相当于单独磁盘的 RAID 0；Mirror 模式相当于 RAID 1，

会将所有数据复制到两块或三块物理盘上；Parity 模式则相当于 RAID 5，会跨越多块磁盘通过奇偶方式检测错误，Storage Spaces 对于 NTFS 或 ReFS 文件系统均有效。

如今回想起来，ReFS v1 有一项颇有野心的功能，就是所谓完整型数据流（integrity streams），主要用于对运行中的文件进行检测和纠错，但令人失望的是，它对 Hyper-V 虚拟磁盘不仅无效，而且会对系统造成严重阻碍。因此，在正常运行的 Windows Server 2012 R2 系统总是竭力回避 ReFS v1。而在业已公布的 Windows Server 2016 TP 版本中出现的 ReFS v2，的确有很多改进值得关注。

ReFS 格式的文件系统，较之 NTFS 的一项重要优势是，当意外错误发生之际，主要表现在 Storage Spaces 蓄池在将 ReFS 作为底层硬盘格式时，能够极大改进修复处理过程，因为 CHKDSK 在处理大型 NTFS 卷时，采取的是自然顺序方式，非常耗时，可是 ReFS 卷则效率明显加快，因为它对整个卷采用了多种并行运行方式。

Windows Server 2016 TP 版本中提供的 ReFS v2 还有一项针对 Hyper-V 的重要功能，就是“数据块克隆”（block cloning），它可以优化处理虚拟数据负载，这里需要用到检查点（checkpointing）和快照（snapshot）技

术。具体而言，就是 ReFS 能够将某个文件中的某些整块克隆到另外文件中，将执行一种复制加写入的中间环节，它能够极大地提高系统整体性能，同时有利于减少随机生成的数据垃圾。

ReFS v2 还采用了一种“簇环”技术（cluster bands），用于将数据分组“打捆”，从而有效改进 I/O 性能。为了检测 ReFS v2 的磁盘操作速度。

笔者做了一个简单的实验，即在 NTFS 卷上生成一个新的 127GB 的 VHDX 文件，用时为 12 分 47 秒，而将相同的磁盘（一块 2TB SAS 的磁盘）进行 ReFS 格式化后发现速度基本一样。分析其过程，原来 ReFS 仅仅是对文件分配空间，它并不对磁盘原有数据进行清理。而且，在 ReFS v2 卷上生成任何大小的磁盘时用时都没有明显差别。

顺便说一下，在了解不同格式文件系统的运行速度的实验过程中，笔者在微软网站还发现了一个专门的测速工具，即 DiskSpd，笔者的实验配置为挂接着 4 块 NVMe SSD 磁盘的 Dell R930，分别采取 NTFS 和 ReFS 格式进行比较。笔者的体会是，系统的错误处理和正常运行其实比速度更重要，这也许正是 ReFS v2 的用意所在吧。

❖ 用 Linux 日志运维服务器

▼ 黄冈 陈金莲

Linux 操作系统因其自由软件的特性而在业界占有越来越重要的地位。但 Linux 也有其致命的弱点——对系统的管理工作主要通命令行的方式进行，这使得它的应用比 Windows 麻烦得多，这可能也是制约 Linux 发展的一个重要因素。虽然现在有很多版本的 Linux 把图形界面也做得越来越人性化，但相对于 Windows 而言，在 Linux 环境中图形界面的应用仍是让人觉得牵制了手脚，学习 Linux 的核心还是学习它的命令环境。并且，在熟练的情况下，命令行方式能提高我们的工作效率和准确度。

Linux 系统运维难点

对于 Linux 环境下各种服务器的管理，则是通过对服务器的配置文件进行编辑来实现。Linux 环境下服务器的配置文件是纯文本的，配置选项又非常多，因此，在配置过程中出错是不可避免的事。一旦配置文件出错，在尝试启动服务时，除了语法问题类的错误之外，系统能给出的其他错误提示非常有限，而且有时并不是配置文件本身出错，这样的话，服务能正常启动，但却不能正常工作。这些都给系统运维带来了很大的障碍。

当然，有些类型的服务，比如 DNS，也提供了一些

专门的排错工具，但功能仍然有限且使用复杂，而且也不是所有的服务都有排错工具。于是，找到一个通用的切实可行的方法来辅助运维人员调试服务器，就显得尤为重要。此时，系统日志文件便可大显身手了。

日志文件

日志文件记录了操作系统在什么时候实施了什么操作，以及系统作出了怎么样的反应，无论操作成功还是失败，在日志中都能找到相应的记录。日志文件的产生方式有两种，一种是由操作系统产生，一种是由各自软件自带的日志功能产生。如图 1 所示，从图中的日志内容可以看出，5 月 13 日 11:04:50 时，在 localhost 主机上，tpvmlpd2 的设备类型不支持，从而知道这个设备因为系统不支持而未被启动。

```
[root@localhost log]# tail messages
May 13 11:04:50 localhost tpvmlpd2[4245]: device type not supported
May 13 11:05:05 localhost tpvmlpd2[4250]: device type not supported
May 13 11:05:20 localhost tpvmlpd2[4257]: device type not supported
May 13 11:05:35 localhost tpvmlpd2[4262]: device type not supported
```

图 1 日志记录

要想利用日志文件来对系统进行运维，就必须先对日志文件有个了解。在 Linux 环境中，常见日志文件有以下几个。

/var/log/cron——计划任务日志。

/var/log/dmesg——内核检测过程中产生的信息。

/var/log/lastlog——检测所有账号登录信息。

/var/log/maillog 或 /var/log/mail/*——邮件系统信息日志。

/var/log/messages——记录系统发生的所有错误信息。

/var/log/secure——安全信息日志。

/var/log/wtmp、/var/log/faillog——记录正确登录系统与错误登录系统者的账号信息。

/var/log/httpd/*、/var/log/news/*、/var/log/samba/*——不同网络服务的日志信息记录处。

在服务器运维过程中，主要运用 /var/log/messages 和 /var/log/httpd/*、/var/log/news/*、/var/log/samba/* 等日志文件。要想让日志文件在运维中起作用，还必须先启动日志服务。

Linux 下的日志服务主要由两个守护进程来完成，一个是 syslogd，主要控制系统与网络等服务的日志记录的信息；一个是 klogd，主要控制内核产生的各种问题的日志。用 Service syslog start 命令即可开启日志服务，

syslog 服务开启后，它的两个守护进程都处于运行中。同时，还应该用命令 chkconfig syslog on 来让服务每次开机时都处于运行状态。

日志文件应用实例

下面，我们以 Apache 服务实例来看看如何利用日志文件来实现服务器的运维。

已经在系统中安装了 Apache 服务器的相关软件包，并且对 /etc/httpd/conf/httpd.conf 配置文件进行了基本设置，但在启动或重启服务器的时候却出现“FAILED”，即启动错误，并且系统没有给出任何提示信息（如图 2 所示）。

```
[root@localhost html]# service httpd restart
Stopping httpd:                                     [ OK ]
Starting httpd:                                     [FAILED]
[root@localhost html]# service httpd start
Starting httpd:                                     [FAILED]
[root@localhost html]# vim /etc/httpd/conf/httpd.conf
[root@localhost html]# service httpd restart
Stopping httpd:                                     [FAILED]
Starting httpd:                                     [FAILED]
[root@localhost html]# service httpd status
httpd is stopped
[root@localhost html]# cat /var/log/message
```

图 2 httpd 服务无法启动

此时，要想通过查阅配置文件去进行错误修正，无异于大海捞针，而且丝毫没有头绪。但是，如果借助日志文件来判断故障点便显得很轻松了。用任何的文本编辑工具都可打开 /var/log/httpd 日志文件进行分析，但最好利用 tail 命令来打开为宜。因为任何一个日志往往包含很多条目，把所有的条目都呈现出来不利于日志分析，而 tail 命令默认只把日志的最后十条显示出来，以利于观察日志的最新情况（如图 3 所示）。

```
root@localhost:~# tail -n 10 /var/log/httpd/error_log
[Fri Jan 23 18:08:31 2015] [notice] SELinux policy enabled: httpd running as context root/systemd
[Fri Jan 23 18:08:31 2015] [notice] suEXEC mechanism enabled (wrapper: /usr/sbin/suexec)
[Fri Jan 23 18:08:31 2015] [notice] Digest: generating secret for digest authentication ...
[Fri Jan 23 18:08:31 2015] [notice] Digest: done
[Fri Jan 23 18:08:31 2015] [notice] Apache/2.3.3 (Red Hat) configured -- resuming normal operations
[Fri Jan 23 18:08:38 2015] [error] [client 192.168.34.133] Directory index forbidden by Options d
[Fri Jan 23 18:08:38 2015] [error] [client 192.168.34.133] File does not exist: /var/www/html/for
[Fri Jan 23 18:08:44 2015] [error] [client 192.168.34.133] Directory index forbidden by Options d
[Fri Jan 23 18:08:44 2015] [error] [client 192.168.34.133] Directory index forbidden by Options d
[Fri Jan 23 18:08:44 2015] [notice] caught SIGTERM, shutting down
```

图 3 httpd 的日志文件

从日志文件可以看出，系统的 SELinux 策略是打开的，并且提示 httpd 服务的主目录 /var/www/html 中的某些文件未找到或权限不够等，而实际上这个文件确实存在于目录中。下面我们就从分析主目录的 SELinux 策略着手。

用 ls -Z /var/www/html 命令来查看该目录下文件的 SELinux 策略，结果如图 4 所示。

```
[root@localhost httpd]# ls -Z /var/www/html
-rw-r--r-- root root root:object_r:user_home_t index.html
```

图 4 目录 /var/www/html 的 SELinux 策略

可以看出，默认首页 index.html 的 SELinux 策略属性为 user_home_t，而需要 httpd 进程能访问则相应的文件及目录必须要是“httpd_user_content_t”或 httpd_sys_content_t 属性才行（关于 SELinux 的策略不是本文要讨论的范畴）。


清楚故障原因后，解决方案就有了。根据复杂程度的不同，可以有以下两种解决方案。一是，通过命令 `chcon -R -t httpd_sys_content_t /var/www/html` 来修改 httpd 进程相关文件及目录的属性。用这种解决方案需要对 SELinux 策略有一定的认识才行。另一种解决方案

比较简单直接，直接用命令 `/usr/sbin/setenforce 0` 来关闭 SELinux 功能，这种解决方案虽然简单，但会降低系统的安全性。

无论用上面哪种方式清除故障后，再用命令 `service httpd start`，则 httpd 又能重新启动，Web 服务器又能重新正常工作了。

上例只是日志文件在服务器运维中应用的一个代表，但由此可以看出，当启动服务时，系统无法给出足够的信息让我们进行服务器运行的故障排除时，藏在系统背后的日志文件可以让运维者找到出路。

Windows 10 实用技巧

 威海 赵永华

重置 Windows 背景

虽然 Windows 10 登录界面布局和样式都不错，但并没有提供更换登录背景图片的功能。笔者在这向给大家介绍一款名为 W10 Logon BG Changer 的小工具，能轻松修改 Windows 10 的登录背景图片。W10 Logon BGChanger 提供两种方式进行修改，分别是使用电脑中的图片和使用单独的颜色，图片支持大部分格式，并可调整图片分辨率。选择好图片后，整个 Windows 10 的登录背景就会换成所选图片。另外一种是要配合当前的 Windows 10 主题，自己选择相对应的颜色。

下载地址：<http://www.greenxf.com/soft/74915.html>。

修改 Windows 10 主题色

在 Windows 10 中虽然可以修改主题颜色，但系统自带颜色较少，要想更换其他颜色就无能为力。此时我们可以利用一款名为 Win 10 ColorControl 的软件，将 Windows 10 设置成任何颜色。Win 10 ColorControl 可以分别设置窗口边框以及任务栏、开始菜单的颜色。颜色可任意，但一定要勾选最下边的“DISable newauto-coloraCCentalgorithm”，否则系统会自动使用与你自定义颜色差不多的系统配色。当颜色都选择好后，点击

“Apply”按钮完成设置，系统就会自动将配色修改成你自己所选的颜色。

Win 10 ColorControl 下载地址：http://www.pc6.com/softview/SoftView_164671.html。

升级到 Windows 10 之后如何删除旧系统冗余文件

通过系统升级成为 Windows 10 之后，Windows 10 考虑到有人还准备要恢复到原来的老系统，所以在升级过程中自动保留下了之前操作系统的文件和数据。保留老系统文件占用空间最大的就是 Windows.old 文件夹，这个文件夹的主要内容是之前操作系统 Windows、Program Files、Useis 三个主文件夹的总和，一般会在 10GB 以上。该文件夹受操作系统保护，很难直接将它删除，此时可以采用磁盘清理来清除。

打开“此电脑”，右击 C 盘选择“属性”，点击旁边的“磁盘清理”按钮。在弹出的对话框中点击“清理系统文件”，系统开始计算 C 盘上可供释放的磁盘空间。计算完毕后，可以看到除了以前 Windows 安装占用空间外，还有若干空间的“临时 Windows 安装文件”。勾选好要清除的项目。然后点击“确定”按钮，稍后系统会再次询问你是否要删除这些文件，点击“确定”即可完

成清除。

另外, Windows 10 本身自带了二十多个普通用户平时根本用不到的文件, 如 XBOX、ONENOTE 等, 通过常规手段无法进行删除, 此时可借助第三方应用, 比如 10AppsManager。

下载地址 <http://pan.baidu.com/s/1hqKuCXu>。

关闭 Windows 10 操作中心

从 Windows 7/8.1 升级到 Windows 10 的用户, 不太习惯全新的操作中心, 原因是这项功能经常弹出各种系统和应用消息, 因此很想关闭操作中心。

在 Cortana 搜索栏输入 regedit 进入注册表编辑器后, 定位到 HKEY_CURRENT_USER\SOFTWARE\Policies\Microsoft\Windows\Explorer (若没有 Explorer 项, 可自己新建一个), 在 Explorer 中新建 “DWORD (32 位) 值”, 重命名为 “DisableNotification Center”, 然后双击 DisableNotificationCenter, 将数值数据改为 “1”, 然后重启电脑, 操作中心就彻底消失了。

解决 Windows 10 下 IE 运行时频繁提示 “Internet Explorer 已停止工作”

在 IE 浏览器中找到 “工具”, 打开 “Internet 选项”, 切换到 “高级” 选项, 在 “设置” 窗格中向下滚动设置项, 找到 “浏览” 区域的 “启用第三方浏览器扩展” 以及 “启用自动崩溃恢复” 选项, 取消勾选, 确定后关闭窗口, 重启系统即可。

禁用 Windows 10 的追踪功能

Windows 10 新增了一个追踪用户使用习惯的服务, 这会暴露用户隐私, 但时在 Windows 10 并没有关闭该服务的功能。如果想要将这些追踪功能给关闭, 可用一款名字为 Remove Windows 10 Spying Features 的小软件, 利用它就可以快速禁用 Windows 10 的追踪功能。

下载地址: <http://www.greenxf.com/soft/75107.html>。

为 Windows 10 文件资源管理器 “整容”

Windows 10 中的文件资源管理器, 界面和功能与以前相比有很大区别, 很多人不习惯。我们可以根据自己

的习惯对 Windows 10 的文件资源管理器进行定制, 用起来就会得心应手了。

比如在 Windows 10 的资源管理器顶端有一个快捷工具栏, 本意是方便用户快速对文件进行某些操作, 但默认只有 “属性”、“新建文件夹” 两个工具按钮, 如果想多添加几个常用的工具按钮, 可以点击后面的向下三角形按钮, 在弹出的 “自定义快速访问工具栏” 中勾选要添加的工具按钮, 如 “删除”、“恢复” 等。

如果你想要添加的功能没有出现在这个菜单中怎么办? 我们可以在其他地方找到想要的工具按钮图标, 直接把鼠标放上去右击就会弹出一个对话框, 点击 “添加到快速访问工具栏” 的子选项就大功告成了。

在 Windows 10 中一打开文件资源管理器, 就默认自动打开了 “快速访问”, 而不是我们习惯的 “我的电脑”, 当然这在 Windows 10 里叫 “此电脑”, “快速访问” 是 Windows 10 新增加的功能, 讨厌它的用户觉得最近使用过的文件夹和文件都会显示在 “快速访问” 里, 自己打开过的歌曲、视频、文档统统都给显示出来了, 这样很容易泄露隐私。其实我们可以修改过来, 只要在文件资源管理器中点击 “查看” 菜单, 选择 “选项” 按钮, 在弹出的 “文件夹选项” 对话框中, 将 “打开文件资源管理器时完成以下操作” 修改为 “此电脑” 就可以了。

另外, 为了保护隐私, 还可以设置 “快速访问” 不显示最近使用的文件, 在对话框中, 点击 “常规” 标签下的 “隐私” 选项。然后不勾选在 “快速访问” 中显示最近使用的文件和常用文件夹即可。同时你也可以点击最下方的 “清除文件资源管理器历史记录” 旁边的 “清除” 按钮, 一键清理掉当前最常使用文件列表, 保证个人隐私不被泄露。

让 Windows 10 账户只能打开指定应用

通过 Windows 10 的 “分配访问权限” 功能, 可轻松实现让某些账户在特定设备访问单独应用。具体操作方式为: 在主账号中进入 “设置→账户→家庭和其他用户”, 点击 “将其他人添加到这台电脑”, 输入该账户电子邮件或电话号码, 点击 “下一步”, 验证成功后, 专用账户添加完成。回到 “家庭和其他用户” 界面, 点击 “设置分配的访问权限”, 选择想要这个账户启动的应用, 使用这种方法设定的专门账户登录后, 只会打开特定应用, 并且全屏显示。

让虚拟服务器时间同步

山东 王学谦 路庆刚

应用环境

笔者所在单位是一所集医疗、教学、科研于一体的大型综合性医院。随着医院规模的不断扩大、医院信息化建设逐步深入，越来越多的需求被提出，而且伴随着各科室要求的不断提高，医院内部的信息系统在数量和复杂程度上都呈级数上升。由于各种应用系统的增多，原来购置的传统服务器在数量上和性能上都无法满足应用系统的增长需求了，而且日益增多的服务器增加了网管人员的日常运维工作量，也造成了中心机房的环境能耗不断攀升，耗费了大量的人力、财力和物力。

结合上述问题，院方基于 VMware vSphere 平台，针对中心机房的服务器区域进行了虚拟化改造。经系统迁移改造后，院内各应用系统在虚拟化平台上运行正常，并且 vCenter Server 基于可视化的管理方式，大幅简化了各应用系统的运维管理和扩展操作，虚拟化改造的成果初步显现。

时间同步需求

经过一段时间的运行，笔者在对院内各科室反馈的系统使用问题归纳时发现，不少科室反映的应用系统故障，根源都集中在了“系统时间不同步”的问题上，问题表现在，应用系统在上线初期系统时间正常，用一段时间后，服务器系统时间与北京时间相比出现延迟变慢，而且随着时间推移，偏差逐渐增大)。再仔细分析一下这些“问题系统”的共同点，服务器都运行在虚拟化平台上。由此，笔者推断问题就出在 VMware vSphere 平台虚拟的那些应用服务器上。

由于在单位中心机房进行虚拟化改造之前，各系统使用独立的机架式物理服务器时，笔者也遇到过类似的问题，当时的解决方式是在内网中配置建立了 NTP 服务器（设置了安全策略，与国家授时中心保持时间同步）。另外，笔者单位的各个应用服务器的 OS 基本上微

软的产品，只需要在服务器控制面板上设置“日期和时间→Internet 时间”，勾选“与 Internet 时间服务器同步”，填上内网的 NTP 服务器的 IP 地址，确定完成后就万事大吉了。

笔者想当然地认为虚拟服务器和物理服务器的时间同步机制都是类似的，基于这种思路，当即对这些有问题的虚拟服务器进行了时间同步配置。

然而好景不长，第二天一上班，就收到了临床科室的反馈：系统时间又变慢了。冷静下来，仔细观察了这些问题虚拟机的时间同步情况，发现按照原来的思路在 Windows 操作系统下设定 NTP 同步后，在刚刚同步完成时，系统时间是正确的，过 1 小时左右再看，时间就变慢了，如图 1 所示。

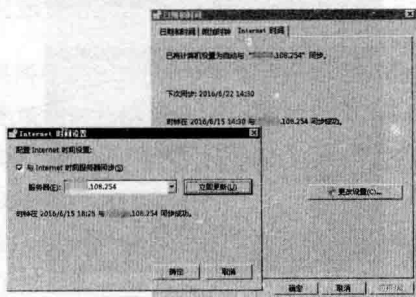


图 1 Windows 操作系统下设置 NTP Server 自动同步

配置实现

通过查阅资料，结合单位服务器的实际情况，配置实现了虚拟化平台下各个应用服务器的时间自动同步，配置过程介绍如下。

单位使用的虚拟化平台是基于 VMware vSphere 5.0 构建的，下面归纳一下在该版本下基于 NTP Server 配置实现虚拟机时间同步的方法。

1. 使用 vSphere Client 连接 vCenter Server，然后在群集中选择需要设置的 ESXi 物理主机，并选择“配置”标签页，接着选择“软件→时间配置”。

2. 选择“时间配置”右侧的“属性”，打开时间配置界面。

3. 选中“NTP 客户端已启用”，点击“选项”。在弹出的“NTP 守护进程 (ntpd) 选项”页面中，点击“常规”选项，在“启动策略”项中，建议选择“与主机一起启动和停止”。

4. 在该页面设置“NTP 设置”，添加 NTP 服务器（NTP 服务器可以添加多个，在笔者单位 NTP 服务器都是工作在内网并且路由可达的），添加后需要选中“重启 NTP 服务以应用更改”，点击“确定”按钮。

5. 待 ESXi 主机与 NTP Server 时间同步后（经笔者测试，在 ESXi 主机的时间同步任务执行完成后大约 15 分钟左右，才能与 NTP Server 自动同步时间），为运行在 ESXi 主机上的虚拟机设置时间同步。前提是，该虚拟机已成功安装并运行了 VMware Tools。在虚拟机 OS（以 MS 阵营的 Windows Server 为例）中桌面右下角找到“VMware Tools”图标，右键单击该图标并选择“打开 VMware Tools”，在弹出的“VMware Tools 属性”窗口，选择“选项→其他选项”，选中“在虚拟机和 ESX Server 之间进行时间同步”，应用确定后，稍后即可实现虚拟机系统时间与 ESXi 主机时间自动同步，如图 2 所示。

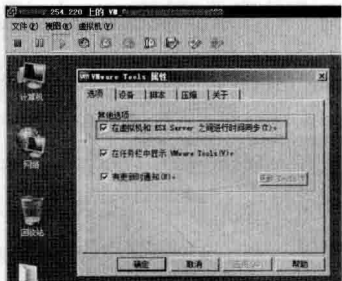


图 2 在 ESXi 上的虚拟机 OS 中设置时间同步

应用效果

经过上述配置过程，在笔者单位的内网中，基于 NTP Server 实现 VMware ESXi 主机中各虚拟机时间自动同步的功能基本实现，能够达到 ESXi 主机先与 NTP Server 进行时间同步，各虚拟机（应用系统服务器）与 ESXi 主机进行时间同步，效果如图 3 所示（运行在 ESXi 之上的各虚拟服务器 OS 系统时间与内网 NTP Server 时间保持自动同步）。至此，笔者经过一段时间的运行观察，单位各科室未再反映应用系统出现时间不同步的故障，达到了预期效果。

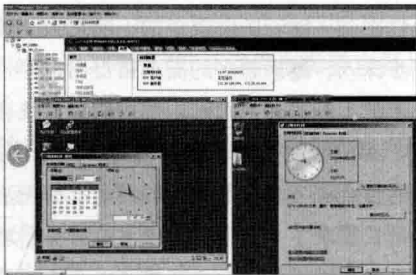


图 3 时间自动同步的执行效果

笔者附注：如果各位读者在为 ESX/ESXi 主机配置 NTP 过程中出现了故障，可以参考 VMware 官方知识库的文档“Troubleshooting NTP on ESX and ESXi 4.x / 5.x / 6.x (1005092)”，链接地址 https://kb.vmware.com/selfservice/microsites/search.do?language=en_US&cmd=displayKC&externalId=1005092。

为 Windows 2012 指定授权服务器

河北 王春海

在 Windows Server 2008 R2 的终端服务中，可以手动指定授权服务器，而在 Windows Server 2012 R2 中，默认只能通过“远程桌面连接服务”管理器，指定授权

服务器。而要使用远程桌面连接服务管理器，则需要安装一系列的组件。但大多数的时候，我们只是想配置一台“远程桌面会话主机”，不想要安装“远程桌面网关

服务”、“远程桌面 Web 代理”这些组件。

那么,有没有办法和 Windows Server 2008 R2 一样,为 Windows Server 2012 R2 的“远程桌面会话主机”手动指定授权服务器呢?本文将介绍这一内容。

在本示例中,Active Directory 的域名是 heuet.com,Active Directory 服务器的 IP 地址是 172.16.17.1,我们在这台主机上安装了“RD 授权服务”,并已经安装许可。在网络中有另外一台 Windows Server 2012 R2,已经加入到域,并安装了“RD 会话主机服务”。接下来,我们在这台 Windows Server 2012 R2 指定“RD 授权主机”。

安装远程桌面会话主机

1. 在准备用作 RD 会话主机的计算机上,打开“服务器管理器”,选择“添加角色和功能”;在“选择安装类型”对话框,选择“基于角色或基于功能的安装”;在“选择角色服务”对话框,选择“远程桌面服务”。

2. 在“远程桌面服务→选择角色服务”对话框,选中“远程桌面会话主机”(如图 1)。

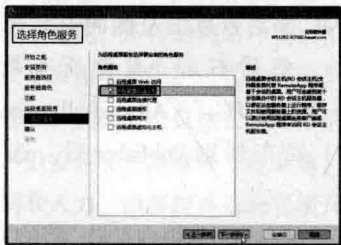


图 1 远程桌面会话主机

3. 安装完成后,重新启动,再次进入系统之后,打开“RD 授权诊断程序”,可以看到,当前远程桌面会话主机没有指定 RD 授权服务。

修改本地策略指定授权服务

接下来在这台计算机上,执行 gpedit.msc,修改组策略,主要步骤如下。

1. 打开“本地组策略编辑器”,在“计算机配置→管理模板→Windows 组件→远程桌面服务→远程桌面会话主机→授权”中,双击右侧的“使用指定的远程桌面许可证服务器”。

2. 在“使用指定的远程桌面许可证服务器”对话框中,选中“已启用”,并在“要使用的许可证服务器”

文本框中,输入 RD 授权服务器的计算机名或 IP 地址,在此输入 172.16.17.1 (如图 2)。



图 2 指定 RD 授权服务器

3. 在“设置远程桌面授权模式”对话框,选中“已启用”,并在“指定 RD 会话主机服务器的授权模式”下拉列表中选择“按用户”。之后,单击“确定”按钮,完成设置。

关闭本地组策略编辑器,打开命令提示窗口,执行 gpupdate /force,刷本地策略。

再次打开“RD 授权诊断程序”,可以看到当前 RD 会话主机已经指定并连接到 RD 授权服务。

修改组策略指定授权服务

如果网络中有多台 RD 会话主机,管理员也可以通过修改系统默认的组策略,为终端服务器统一指定 RD 授权服务,这样就不需要再在每台 RD 会话主机一一配置。主要步骤如下。

1. 在 Active Directory 服务器中,打开“组策略管理”,右击“Default Domain Policy”,选择“编辑”(如图 3)。



图 3 编辑默认域策略

2. 在“计算机配置→管理模板→Windows 组件”中双击“远程桌面服务”,在“远程桌面服务→远程桌面会话主机→授权”中,双击右侧的“使用指定的远程桌面许可证服务器”。之后的配置则与在单机配置相同,不一一介绍。

3. 在服务器上打开“RD 授权管理器”，可以看到已经安装及分配的许可。

4. 当有 RD 会话主机分配许可之后，在“已颁发”

列表中可以查看。

此后，凡是加入到域中的 RD 会话主机则会自动指定 RD 授权服务器。



用 AppLocker 设置控制策略

威海 赵永华

AppLocker 最早出现在 Windows 7 系统中，是一项所谓“应用程序控制策略”的安全功能。利用 AppLocker，管理员可以方便地配置控制用户在计算机上可运行哪些程序、安装哪些文件、运行哪些脚本。

由于 AppLocker 是基于组策略管理和配置的，因此我们很容易将其部署到整个网络环境中。AppLocker 同样能够在 Windows Server 2008 R2 中发挥作用。

在 Windows Server 2012 R2 中配置 AppLocker

AppLocker 替代了之前版本的软件约束策略 SRP (Software Restriction Policies)，在配置方面也更为简便。这里笔者介绍的是在本地计算机上对 AppLocker 进行配置，但是大家通过活动目录组策略 ADGP (Active Directory Group Policy) 很容易应用到多部机器之上。具体操作方式如下。

1. 登录 Windows Server 2012 R2，以管理员身份启动控制台程序 MMC。

2. 从列表中选择组策略 Group Policy 后点击“添加”，然后从快照 (snap-ins) 列表中选择服务 Services，点击“OK”。

3. 在 MMC 控制台左侧，依次展开项目 Local Computer Policy → Windows Settings, Security Settings → Application Control Policies → AppLocker，右击执行规则 Executable Rules 后从菜单中选择生成默认规则 Create Default Rules，即可以看到可运行所有文件的管理员组 Administrators Group 成员。

4. 重复上述操作，即可设置系统安装规则 Windows

Installer Rules，脚本规则 Script Rules，以及应用包件规则 Packaged app Rules。

利用 AppLocker 阻止用户安装程序实例

比如管理员不允许用户擅自安装浏览器 Google Chrome，为此，管理员首先下载其安装包 Google Chrome.msi，然后执行以下步骤。

1. 在 MMC 控制台点击左侧的安装规则 Windows Installer Rules，然后右击“允许所有数字签名的 Windows 安装程序” (All digitally signed Windows Installer files) 发布规则 Publisher 后，选择“属性” (Properties)。

2. 在“所有属性”对话框内点击“例外” (Exceptions) 栏目，确保“发布”选项选中后点击“添加”，然后通过浏览方式找到 Google Chrome 说明文件。

3. 在“打开”对话框中选中 .msi 文件后点击“打开”，在“发布例外”对话框移动选中 Google Chrome，点击“OK”。

4. 在 MMC 窗口右点 AppLocker 后选择“属性”，在“强制” (Enforcement) 栏目中勾选相应规则后点击“OK”。

5. 为了让设置生效，在 MMC 控制台点击面板左侧的“服务” (Services)，在服务列表中定位 Application Identity，双击之。

6. 在属性对话框内的“通用”栏目下，将启动类型服务设置为自动方式 (Automatic)，在服务状态下点击“启用” (Start) 后点击“OK”。

经过上述设置，当用户试图安装谷歌浏览器时，就会被 AppLocker 阻止，显示信息如图 1 所示。

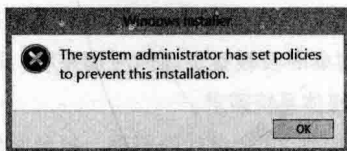


图1 程序运行被 AppLocker 阻止界面

经验总结

AppLocker 能够为系统管理带来很多便利, 通过使用动态规则, 可以阻止不同类型的影响系统安全的应用程序(从游戏到恶意软件等)侵入, 还可以仅允许批准的应用程序在网络中执行。



桌面虚拟化构建电教室

贵阳 朱红军

传统教室多媒体系统存在的问题

随着信息化的不断发展, 学校的教学模式也发生了深刻变化, 教师的教学普遍已经从板书教学转变为多媒体教学, 多媒体技术的引入又给管理人员带来了新的问题, 由于学校信息化建设一般都分步实施导致计算机的配置、型号各不相同, 所处的网络环境也相当复杂。传统的管理模式是采用硬盘保护(实时还原)和网络同传等方法进行管理, 这些方法虽然在多媒体系统的可用性得到了提高, 但安装和更新软件非常麻烦, 而且需要耗费大量的时间和人力, 给多媒体系统管理人员带了极大的困难, 甚至严重到影响正常的教学秩序。主要表现在以下方面。

1. 管理人员少, 维护时效长。

多媒体教室数量多, 且分布在校园的多个建筑楼层, 特别是在产品质保期后出现问题频率较高且时间也相对集中, 但管理人员少, 很难及时解决实际问题。

2. 硬件配置不统一, 增大维护难度。

由于学校的信息建设周期不同, 就导致不同时期采购的计算机硬件配置不一, 即使采购初期是一致的, 在使用一段时间后也会更换配件, 造成计算机配置也不会完全相同。

3. 软件安装与更新难

因课程教学实际需要和教师个人需求的不同, 每间教室的计算机系统中所安装的软件程序和版本也有差别, 程序之间极易产生冲突, 难以满足教学需要。

4. 公众化使用, 病毒难以防护。

网络与移动存储设备的广泛使用, 造成病毒的迅速传播, 防不胜防。虽然安装有杀毒软件, 但病毒库更新滞后, 难以确保系统安全。

5. 计算机耗能高, 浪费能源。

一所学校都会有几间多媒体教室, 平均每台电脑 200W 以上的耗电, 产生的能耗, 均不符合绿色环保的要求。

基于传统教室多媒体系统当前存在的不足, 通过对桌面虚拟化新技术的学习, 提出运用桌面虚拟化技术到教室多媒体系统的管理中来, 将有效地解决这些问题。

桌面虚拟化技术分析

在传统教室多媒体系统管理中, 通过人力和强化管理可以在一定程度上缓解在其维护与使用上的突出矛盾, 但效果并不理想。近几年来, 逐渐兴起的虚拟化技术, 可以有效地解决这些问题。

作为虚拟化核心技术之一, 桌面虚拟化技术(Desktop Virtualization)可以在不影响用户终端的前提下, 方便地实现教室多媒体系统的集中化管理, 减轻维护工作量, 并且可以有效地降低建设和运维成本。

桌面虚拟化是指将计算机的终端系统(也称作桌面)进行虚拟化, 以达到桌面使用的安全性和灵活性。可以通过任何设备, 在任何地点, 任何时间通过网络访问属于我们个人的桌面系统。它依赖于服务器虚拟化, 在数据中心的服务器上进行服务器虚拟化, 生成大量的独立

的桌面操作系统（虚拟机或者虚拟桌面），同时根据专有的虚拟桌面协议发送给终端设备。用户终端通过以太网登录到虚拟主机上，只需要记住用户名和密码及网关信息，即可随时随地的通过网络访问自己的桌面系统，从而实现单机多用户。

桌面虚拟化的优势

桌面虚拟化与传统 PC 架构的教室多媒体系统相比较，主要表现在以下五大优势。

1. 更灵活的访问和使用，用户对桌面的访问不需要被限制在具体设备、具体地点和具体时间。我们可以通过任何一种满足接入要求的终端设备，就可以访问我们的主计算机桌面。

2. 更广泛与简化的终端设备支持，由于所有的计算都放在服务器上，终端设备的要求将大大降低，不需要传统的台式机，而瘦客户端又重新回到我们的视野，而且智能手机、上网本、接近报废的 PC 等设备，甚至于电视，都成为可用设备。在虚拟桌面的推动下，未来的企业 IT 架构，可能会更像一个电视网络，变得更加灵活，易用。

3. 终端设备采购、维护成本大大降低，这种 IT 架构的简化，带来的直接好处就是终端设备的采购成本大量降低。

4. 集中管理、统一配置，使用安全。由于计算发生在数据中心，所有桌面的管理和配置都在数据中心进行，管理员可以在数据中心进行对所有桌面和应用进行统一配置和管理，所有的数据和计算都发生在数据中心，则数据和信息不需要通过网络传递，增加了安全性。另外，这些数据也可以通过配置不允许下载到客户端，保证用户不会带走、传播保密信息。

5. 降低耗电、节能减排。传统 PC 一般在 200W 以上，而瘦客户端在 25W 左右，耗电量接近十分之一。所以，一年的电费也会降低 90% 左右。而耗电的减少，也意味这碳排放的减少，达到学校创建节能型校园的目标，同时也适应低碳时代的社会发展要求。

实施方案

通过一台基于超融合架构服务器，集运算、储存、

网络为一体的结构，便于灵活扩展、完全依靠软件驱动的 IT 环境的桌面云教室多媒体应用系统，以满足日常各教室对多媒体系统需求。

采用“N+1”冗余设计的原理，每台服务器实际承担 60 个用户的多媒体教学需求。

1. 部署环境

VMware View 6，VMware vSphere 6。

2. 主要配置

硬件：超融合服务器（CPU：2 颗 Intel Xeon Processor E5-2690 v4 14C 2.6GHz 35MB Cache 2400MHz 135W；MEM：256GB；SSD：2 块 400GB；HDD：6 块 1.2TB SAS；Network：2 个 10Gb 光口）、光纤交换机等。

软件：教育版 VMware vCenter Server 6、教育版 VMware vSphere6、教育版 VMware Horizon。

桌面操作系统：Windows 7/8。

3. 主要应用：教师课堂教学、学术讲座。

该架构搭建完成之后，终端用户能够通过前端瘦客户机方式连接到运行在学校数据中心的桌面。

VMware View 6 打破了软件、硬件和操作系统之间相互依赖的关系，使得 IT 管理员无需在每个终端用户的设备上实际安装或管理桌面环境。通过一个中央位置，IT 部门只需数分钟内即可交付、管理和更新所有 Windows 桌面和应用程序。

VMware View 使应用程序和桌面的测试、部署和支持变得更加容易，成本也大幅降低。

经验总结

基于超融合服务器架构的桌面虚拟化所具有的五大优势，给我们学校多媒体系统的使用与维护带来了全新革命。桌面云虚拟化技术为我们提供了切实可行的解决方案，它的价值将随着应用不断的体现出来。

伴随着网络速度的提升和“互联网+”教育与基础教育深度融合，桌面虚拟化技术必将实用化到应用实际中，桌面虚拟化本身的理念，也将促进基础教育信息化健康、快速发展。

❖ 虚拟云桌面管控终端

南京 聂明辉

单位日常坐班教工有 500 多人，每人配备一台电脑做办公用。因为单位已经构建了多个业务系统，所以日常的办公都是通过个人电脑进行。由于每个人的使用习惯不同，时间久了个人办公电脑经常会出现各种各样的问题而影响工作。这时候，网络管理中心的电话就会响个不停，大家几乎每天都要往返各个不同的办公场所。而事实上，很多问题都是极其简单的，如此造成了人力资源的极大浪费，办事效率极低。

应用需求

网络管理中心经过开会讨论后，决定彻底解决此问题。首先，将本单位个人办公电脑存在的主要问题进行了归纳，大概包括以下三类：1. 应用问题。如浏览器不兼容以及插件被阻止问题，再如 Office 系统不兼容问题等。2. 网络问题。如个人电脑防火墙配置不当，系统 IP 地址设置不当问题等。3. 安全问题。如被病毒感染或者被木马控制等。归根结底，上述问题都需要对个人办公电脑进行操控修复。而在当前的状况下要进行此项操作只有两种途径：一是上门服务；二是远程控制。上门服务即是我们目前采用的方式，比较浪费时间。远程控制需要远端用户的配合，对用户要求较高，只有极个别用户能做好配合，对大部分用户并不合适。

综上所述，要解决客户机的远程维护问题，我们必须另辟蹊径，重新考虑一套方案，该方案必须简单易行，既能满足用户日常办公的需要，又便于网络管理中心的高效管理。最终，我们考虑部署一套虚拟云桌面系统。

解决方案

所谓虚拟云桌面系统，是指基于云平台的系列虚拟系统，用户通过简单的操作可实现快速地远端登录，获得如同本地电脑一样的操作效果和功能。云平台能够将

所有实体服务器进行资源汇聚整合，形成运算资源池和存储资源池（如图 1 所示）。



图 1 云平台资源池

本例中，我们以七台 IBM 刀片服务器和 50T IBM 存储为基础，构建了强大的资源池。之后，通过模板批量构建虚拟主机（如图 2 所示）。

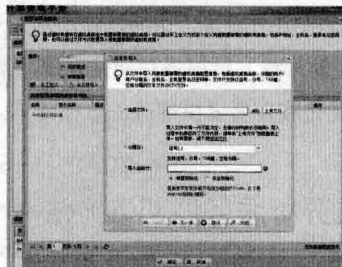


图 2 批量创建虚拟机

批量创建虚拟机，首先需要在模板文件中按照格式要求填写好相关虚拟机信息，模板文件格式（如图 3 所示）。

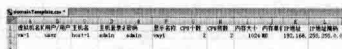


图 3 虚拟机创建模板格式

按照系统提示，将文件导入云平台系统中，所有虚拟机将按照指定参数自动生成（如图 4 所示）。

名称	状态	CPU	内存	磁盘	模板名称
VM-001	运行中	2%	256M	20GB	Windows7-64
VM-002	运行中	1%	256M	20GB	Windows7-64
VM-003	运行中	1%	256M	20GB	Windows7-64
VM-004	运行中	1%	256M	20GB	Windows7-64
VM-005	运行中	1%	256M	20GB	Windows7-64
VM-006	运行中	1%	256M	20GB	Windows7-64
VM-007	运行中	1%	256M	20GB	Windows7-64

图 4 批量生成的虚拟机系统

因为在模板文件中我们已经配置好了相应的登录账号和 IP 地址,所以生成后的虚机便可以直接联网使用了。在云平台管理端,每台虚拟机都会对应生成一个快速链接图标,该图标可以复制到任一用户终端机上。

单机链接图标,输入对应的账号和密码,即可登录虚拟云桌面系统。

在虚拟云桌面,可以实现所有与本地系统相同的办

公操作,包括编辑文字、拷贝文件、打印文档等。

当虚拟云桌面出现问题时候,如浏览器设置不当或者 Office 文档错误等,网络管理中能够从云管理平台直接登录桌面系统,进行相关维护,包括升级软件、重装系统、设置浏览器、配置 IP 地址等。实现了客户端电脑问题的快速处理,大大提高了网络管理中心的办事效率。

构建 Web 日志分析服务器

新疆 马小川

随着 Web 网站的发展和规模不断扩大,对于网站日志进行分析越来越重要。在 Web 服务器日志中,记录了 Web Server 接收请求以及运行状态的各种原始信息。对这些信息进行统计和分析,能够有效地掌握网站的运行状况,了解网站访问量、访问高峰时段、访问返回错误等信息,帮助运维人员加强对网站系统的维护和管理,为网站持续优化和发展提供准确的数据依据。

Web 日志分析服务器部署方法

Web 日志分析是通过分析工具的处理,将日志文件中包含的各种原始信息进行分析和统计,最终得到对运维人员有帮助的数据。日志分析有两种架构形式,一种是在 Web 服务器上安装日志分析程序,日志分析就在 Web 服务器上完成。另一种是将 Web Server 的日志文件通过网络传送到专门的日志分析服务器上,在日志分析服务器上完成日志分析。

对于小型网站而言,日志分析工具可以和 Web 服务器放在一台服务器上运行。但对于大中型网站,由于网站为了提高并发服务能力,都采用前端负载均衡技术,并发的情况会有多台服务器产生 Web 日志。对于 Web 日志,由一台专用的 Web 日志分析服务器来进行日志的集中收集和统计分析比较合适。将日志分析工具安装在专门的日志分析服务器上,也避免了因日志分析给 Web 服务器带来运行负担。

本文将介绍第二种日志分析服务器的部署方法,即采用一台专门的日志分析服务器来进行 Web 日志分析的方式(如图 1 所示)。

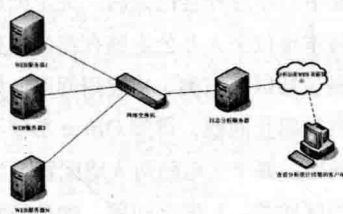


图 1 日志分析服务器网络架构

Web 日志分析原理

Web 服务器日志记录了 Web Server 接受请求以及运行状态的各种原始信息。在 WWW 服务中,客户端访问网站,向 Web 服务器发送请求,根据 HTTP 协议,这个请求中包含了客户端的 IP 地址、浏览器的类型、请求的页面等一系列信息。Web 服务器端收到客户端请求后,将其要求的信息返回到客户端。如果出现错误,将返回错误代码;Web 服务器端将访问信息和错误信息都记录到日志文件中。

通过对日志文件中所包含的信息进行统计和分析,就能有效地掌握网站的运行状况,了解访问分布,帮助诊断错误等。对日志中访问时间的统计分析,可以得到网站在某段时间内,访问的高低峰值;对请求页面的统

计分析，可以知道访问者对哪些页面内容最感兴趣，对哪些内容不感兴趣，从而可以对网站内容进行相应的改善和调整；对访问者 IP 进行统计，可以了解是哪些人在访问网站；对错误信息进行分析，可以了解网站访问存在哪些问题，并予以改正。

对于搭建 Web 日志分析服务器，需要考虑日志提取、定时执行提取任务、日志分析这三个方面的问题。

日志提取，是指在 Web 服务器中的日志文件，需要被传送到日志分析服务器上进行分析处理。

定时执行，是指网站访问记录不断在生成，每天在 Web 服务器访问量最低的时候，定时执行日志提取任务，既可以满足日志分析工作的需要，又可以最大限度地减轻日志提取对服务器的影响。

日志分析，是指日志分析服务器上安装日志分析软件，日志分析软件对从 web 服务器上提取来的 Web 日志进行分析，并用 Web 页面的方式呈现。

本文采用 rsync、cron 和 AWStats 来解决 Web 日志分析服务器的日志提取、定时执行和日志分析问题。为了说明原理，这里只以一台日志分析服务器和一台 Web 服务器的最简架构为例进行阐述 Web 日志服务器的部署原理（如图 2 所示）。其中，Web 服务器使用 Apache 服务器，网站域名为“www.mxctest.com”，IP 地址为“192.168.2.1”；日志提取使用 rsync 软件，采用文件同步的方式快速有效地实现日志文件的提取；使用 Linux 系统自带的 cron 服务定时执行日志提取任务；日志分析工具以 AWStats 为例，日志分析服务器 IP 地址为“192.168.2.2”。

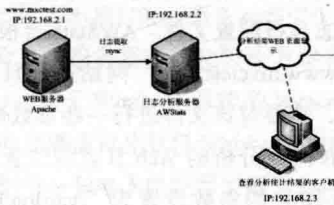


图 2 AWStats 日志分析拓扑图

部署 rsync

rsync（remote synchronize）是一款免费的能够实现远程同步功能的软件，它在同步文件的同时，可以保持原来文件的权限、时间、软硬链接等附加信息。rsync 是用“rsync 算法”提供了一个客户端和远程文件服务器的文件同步的快速方法，而且可以通过 ssh 方式来传输文件，有较高的保密性。

做数据分析的前提是获取日志，AWStats 的实现机制是将 Web 上运行的日志按照指定的格式传送到服务器上进行分析。数据提取的方法有很多，本文使用同步日志的方法，日志分析服务器从 Web 服务器同步日志文件，达到日志提取的效果。同步工具采用 rsync，在 Web 服务器端和日志分析服务器都需要安装 rsync。其中，日志分析服务器作为 rsync 客户端，Web 服务器作为 rsync 服务器端。在日志文件同步过程中，rsync 客户端（日志分析服务器）连接 rsync 服务器端（Web 服务器）开放的服务端口，通过账号口令核查后，进行指定目录的文件同步传输，最终实现客户端与服务端日志文件一致。

1. 在 Web 服务器上安装 rsync

使用 yum 安装 rsync：yum install -y rsync

创建配置文件 /etc/rsyncd.conf，内容如下：

```
uid=nobody
gid=nobody
use chroot=no
max connections=4
pid file = /var/run/rsyncd.pid
lock file = /var/run/rsyncd.lock
log file = /var/log/rsyncd.log
[httpd]
path = /var/log/httpd
comment = BACKUp log
ignore errors
read only = true
list false
auth user = rsyncuser
hosts allow = 192.168.2.2
secrets file = /etc/rsyncd.secrets
```

“rsync.conf”是 rsync 的主配置文件，文件中设置了模块，模块都是以 [name] 命名。模块主要定义了哪个目录要被同步，授权用户名、IP 地址，指定登录密码文件等，rsync 服务器可以根据需要定义多个模块。rsync 客户端根据不同模块名来访问需要同步的目录。本例定义了一个名为“httpd”的模块，该模块中的 path 参数指定了要被同步的目录为“/var/log/httpd”，允许 IP 地址为 192.168.2.2 的客户端能够同步服务器端“/var/log/httpd”下的日志文件。授权同步的用户是 rsyncuser，并且登录密码文件保持在 /etc/rsyncd.secrets 文件中。

创建 /etc/rsyncd.secrtes 文件

rsyncuser.123456

设置 /etc/rsyncd.secrets 文件的权限（必须是 600）。

chmod 600 /etc/rsyncd.secrets

作为 rsync 服务器端，需要运行在 daemon 模式：

rsync --daemon

2. 配置日志分析服务器上的 rsync

作为 rsync 客户端，使用 yum 将 rsync 安装完成后，只需要创建 /etc/rsync.pass 文件，设置内容为：123456，这个密码对应 Web 服务器上 /etc/rsync.secrtes 文件定义的密码。rsync.pass 文件的权限也必须设置为 600，于 rsync.secrtes 文件一致。

rsync 客户端使用如下命令从服务端同步日志，即客户端根据 rsync 服务端主配置文件中 [httpd] 模块定义的访问授权参数，将模块指定目录下的文件同步到客户端的“/var/log/httpd”目录下，实现日志文件从 web 服务器到日志分析服务器的提取：

```
/usr/bin/rsync -vzrtopg --delete --progress
rsyncuser@192.168.2.1:: httpd /var/log/httpd --password-
file=/etc/rsync.pass
```

定时执行工具 cron

cron 是一个 Linux 内置的定时执行工具，可以在无需人工干预的情况下运行作业，类似于 Windows 系统下的“任务计划”。由于 Web 服务器日志文件较大，在网站访问用户量最低的时候进行日志同步，对系统的影响最小。

使用 cron 设置定时执行日志同步任务。vi 编辑 /etc/crontab，写入以下内容：

```
0 3 * * * root run-parts /etc/cron.daily/rsynclog.sh
```

该命令的意思就是每天 3 点执行 /etc/cron.daily 目录下的文件名为“rsynclog.sh”脚本。

而“rsynclog.sh”的脚本文件内容如下：

```
#!/bin/sh
```

```
#rsynclog.sh
```

```
/usr/bin/rsync -vzrtopg --delete --progress
rsyncuser@192.168.2.1:: httpd /var/log/httpd --password-
file=/etc/rsync.pass
```

“rsynclog.sh”文件内容其实就是 rsync 客户端从 rsync 服务端同步日志的命令。通过 cron 工具设置定时执行该脚本文件，实现了日志文件的定时提取。

日志分析工具——AWStats

AWStats (Advanced Web Statistics) 是一个免费的功能强大的服务器日志分析工具，它可以基于服务器日志，创建 Web 统计数据动态分析报告，包括访问量、访问者数量、页面、点击、高峰时段、操作系统、浏览器版本、搜索引擎、关键字、机械访问、无效连接等。数据以可读性强的 Web 方式呈现。AWStats 可以运行在多种操作系统下，可以通过 CGI 或者命令行方式运行。通过即时数据文件，AWstats 可以快速地处理大数据量的日志文件。AWStats 可支持多种 Web 服务器生成的日志格式，包括 IIS, Apache, 自定义等。

AWStats 功能强大，可以通过参数配置实现强大的日志分析功能。关于 AWStats 的安装和配置，网上有较多的配置实例。本文限于篇幅，主要从原理分析出发，仅列出一些基本配置参数和步骤。

首先将 AWStats 安装包解压后，复制到 /usr/local/awstats 目录中。/usr/local/awstats/tools 目录中的“awstats_configure.pl”文件是 AWStats 的安装配置文件。由于 AWStats 是基于 perl 语言书写的程序，所以需要 perl 命令来执行。

执行“perl awstats_configure.pl”命令后，将生成 AWStats 软件安装的交互配置向导，根据该向导的指示，设置需要进行日志分析网站的域名和日志分析配置文件存放路径等信息。在安装配置向导完成后，在“/etc/awstats”目录下会生成名为“awstats.www.mxctest.com.conf”的文件，该文件就是“www.mxctest.com”这个网站的日志分析配置文件。AWStats 会根据这个配置文件，对“www.mxctest.com”网站进行日志分析。因此根据情况，需要对该文件进行一些参数修改。例如，指定 AWStats 需要分析的 Web 日志的位置，本例将配置文件中 LogFile 的参数设置为“/var/log/httpd/access_log”，“access_log”就是日志分析服务器通过 rsync 软件从 Web 服务器中提取而来的 Web 日志。

AWStats 需要 httpd 服务的支持，因此，AWStats 安装配置向导会根据配置情况，对服务器的 httpd 服务配置文件“httpd.conf”进行修改，在该配置文件中添加 AWStats 相应的配置。

将 AWStats 安装设置完成后，在“/usr/local/awstats/wwwroot/cgi-bin/awstats.pl”目录下，执行“perl awstats.pl -update -config=www.mxctest.com”命令，通过该命令对域名为网站日志数据进行统计分析。

在客户机上，访问 <http://192.168.2.2/awstats/awstats.pl?config=www.mxctest.com>，可以通过 Web 页面查看到该网站日志的统计分析结果（如图 3 所示）。网站运维人员通过 Web 页面可以直观地了解网站的运行状况。



图 3 AWStats 日志分析 Web 页面示例

❖ 用 KVM 虚拟化网络服务

▼ 山东 孟秉能 时佃兴

单位的服务器设备大都是 2009 年左右采购的，早已进入淘汰期，受经费的限制，一直没有得到更新。虽然在管理员的精心维护之下，这些设备大部分还在正常运行，但由于单位的门户网站、数据中心、电子邮件等重要服务都安装在这些设备之上，管理维护的压力越来越大。不久前，单位终于购进了两台配置较高的服务器（E5-2620V3×2，64G，1T×6），除有一台必须安装指定服务外，还有一台服务器可以自由支配。怎样将单位重要的网络服务安装在一台服务器上面，同时又要兼顾维护方便呢？笔者不禁打起了服务器虚拟化的主意。

目前，常见的服务器虚拟化解决方案有基于 Linux 系统的 KVM，基于 Windows 系统的 Hyper-V，以及适合任何系统的老牌虚拟化软件 VMware。由于单位的门户网站、数据中心和电子邮件都是基于 Linux 系统，从兼容性和经济性方面考虑，笔者准备采用基于 Linux 系统的 KVM 解决方案。

安装配置 KVM 服务器

KVM 服务器系统我们准备采用最新的 CentOS7，CentOS 是 RHEL（Red Hat Enterprise Linux）源代码再编译的产物，而且在 RHEL 的基础上修正了不少已知的 Bug，相对于其他 Linux 发行版，其稳定性值得信赖。

1. 安装 CentOS 系统

从 CentOS 官方网站下载最新的 DVD 版本，刻录

DVD 光盘或者写入优盘进行系统安装。在安装过程中我们需要注意以下几点：系统默认语言尽量选择英语，如果选择中文，将来使用 VNC 远程管理的时候会出现乱码。软件选择使用“最小虚拟化主机”（如图 1），其他软件需要的时候再安装。手动配置硬盘分区，根据自己的需要，可以为虚拟机划分单独的硬盘空间（比如划分单独的 /data 分区）。

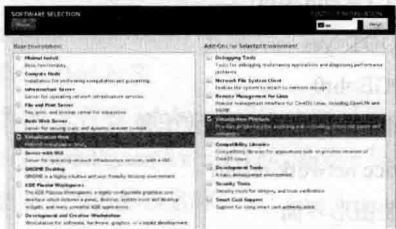


图 1 选择最小虚拟化主机安装模式

系统安装完毕以后，首先运行 `yum update` 更新一下系统，将系统升级到最新，然后运行以下命令，查看是否已经在 BIOS 中开启了 VT。

```
# lsmod|grep kvm
```

如果在命令输出中包含 `kvm 525409 1 kvm_intel` 等字样，说明已经开启了 VT，否则就要重启系统进入 BIOS 进行设置，启动 VT 功能。

2. 配置桥接网络

KVM 虚拟机支持多种网络模式，比较常用的是 Bridged（桥接模式）和 NAT（网络地址转换模式），我

们需要虚拟机具备和独立主机相同的功能，可以与其他机器互相访问，所以在这里我们选择 Bridged（桥接模式）。

（1）复制 ifcfg-enp2s0f0（每台服务器的网卡名称不一样，以自己的名称为准）配置文件为 ifcfg-br0，并将 ifcfg-br0 修改为如下配置：

```
TYPE=Bridge
# 桥接模式
BOOTPROTO=static
DEFROUTE=yes
PEERDNS=yes
PEERROUTES=yes
IPV4_FAILURE_FATAL=no
NAME=br0
DEVICE=br0
ONBOOT=yes
IPADDR=10.7.3.220
# 服务器的 IP 地址
NETMASK=255.255.255.0
GATEWAY=10.7.3.1
# 网关地址
```

（2）原网卡 ifcfg-enp2s0f0 配置文件只需要保留以下内容，其他全部注释掉：

```
NAME=enp2s0f0
DEVICE=enp2s0f0
ONBOOT=yes
BRIDGE=br0
```

（3）重启网络让桥接模式生效

```
# service network restart
```

3. 安装图形界面

作为网络服务器，一般不用安装图形界面，但考虑到使用 virt-manager 在图形界面下管理虚拟机非常方便，加之以后可能需要使用 VNC 远程管理 KVM 服务器，所以安装一个最基本的图形界面还是非常有必要的。

（1）安装 virt-manager 管理工具

```
# yum install virt-manager
```

（2）安装图形界面

```
# yum groupinstall "X Window System"
```

```
# yum install gnome-classic-session gnome-terminal
nautilus-open-terminal control-center liberation-mono-fonts
```

（3）设置系统默认启动图形界面

```
# unlink /etc/systemd/system/default.target
```

```
# ln -sf /lib/systemd/system/graphical.target /etc/
systemd/system/default.target
```

如果不想让 KVM 服务器默认启动图形界面，这一步可以不做设置，当需要启用图形界面的时候，输入 startx 即可。

（4）重新启动系统

```
# reboot
```

服务器重启之后，我们就有一个具备图形界面的 KVM 服务器了。

转化物理机为 KVM 虚拟机

KVM 服务器安装完毕以后，就可以根据需要建立自己的虚拟机了。如何将正在运行的服务器平滑地迁移到 KVM 虚拟机，这是我们面临的一个大问题。所幸，RedHat 已经为我们研发了 virt-p2v 这个将物理机转化为虚拟机的工具，它可以通过 SSH 连接物理机和转化服务器（转化服务器也可以安装在 KVM 服务器上）对目标服务器进行在线迁移。

1. 准备迁移环境

（1）安装转化服务器

```
# yum install virt-v2v
```

转化服务器可以单独安装，也可以和 KVM 服务器安装在一起，为方便起见，我们将转化服务器安装在 KVM 服务器上。

（2）制作 virt-p2v 迁移工具

从这个网站（<http://oirase.annexia.org/virt-p2v/>）下载最新的 P2V 光盘镜像文件，然后刻录光盘或者写入优盘待用。

（3）配置转化服务器 sshd 服务

修改 /etc/ssh/sshd_config 配置文件，并做如下修改：

```
AllowTcpForwarding yes # 允许 tcp 转发
```

```
PermitRootLogin yes # 允许 root 用户登录
```

启动 sshd 服务

```
# systemctl start sshd.service
```

查看 sshd 运行状态

```
# netstat -anput|grep ssh
```

2. 迁移目标服务器

将 P2V 工具光盘或者优盘接入目标服务器，然后设置目标服务器从光盘或者优盘启动，进入 P2V 配置界面（如图 2），输入转化服务器 IP 地址、用户名和密码（在这里我们使用 root 账号），勾选 “Use sudo when running

virt-v2v”，然后点击左下角的“Configure network...”为P2V工具设置一个可用的局域网IP地址。最后，点击“Test connection”检查一下SSH是否可以连接，如果出现“connected to the conversion server”的提示，说明P2V工具已经成功连接到转化服务器。

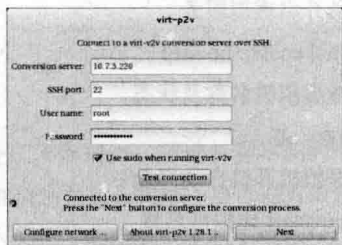


图2 配置连接转化服务器所需账号

点击“next”进入配置虚拟机界面（如图3），在这里我们可以根据自己的实际情况，配置虚拟机的名称、CPU数量和内存大小，勾选需要进行转化的目标服务器上的所有磁盘和网络接口（如果P2V工具使用优盘启动，不要勾选转化优盘）。



图3 配置虚拟机各项参数

需要特别注意的是，在Virt-v2v输出选项卡中，Output to支持很多类型，比较常用的是local和libvirt。如果转化服务器和KVM服务器安装在一起，libvirt选项可以直接生成正常运行的虚拟机；如果你想指定存放路径，手工添加虚拟机，可以选择local类型，然后在Output storage里面指定路径。Output format支持raw和qcow2两种虚拟文件格式，P2V工具默认输出raw格式，不要试图修改输出格式为qcow2，否则会在转化过程中出错。如果想在虚拟机中使用qcow2格式，可以在转化完成后再进行设置。这里我们选择输出类型为libvirt，其他选项保持默认即可，注意勾选“Enable server-side debugging”选项，以便出错时我们可以进行调试工作。

虚拟机配置全部完成后，就可以点击“Start conversion”按钮进行转化了，根据网络速度和硬件配置的不同，转化物理机所需的时间也不尽相同，一般说来，一块300GB容量的磁盘需要转化8-10个小时的时间。

您可以根据自己的实际情况，安排在晚上或者周末进行服务器的迁移工作，尽量减少服务器的宕机时间。一旦迁移工作完成，应该马上关闭目标服务器，如非必要就不要再重新启动它。

登录KVM服务器，会发现我们转化物理机生成的虚拟机已经可以正常运行了，只是它的虚拟文件系统是raw格式，如果需要快照功能，那么qcow2格式也许更加适合你，两种虚拟文件格式的性能差距已经很小，qcow2格式完全可以满足我们的需要。使用如下命令可以将raw格式的虚拟文件转换成qcow2格式：

Qemu-img convert -f raw -O qcow2 raw 文件名 qcow2 文件名

虚拟文件格式转换完成后，记着在虚拟机的虚拟硬件列表中将虚拟磁盘的格式由raw更改为qcow2，然后重新启动虚拟机。

安装配置远程管理工具

到目前为止，我们已经有了了一台正常运行的KVM服务器，通过virt-manager软件，可以在图形界面下完成对虚拟机的克隆、安装、调试和开关机等绝大部分操作。不过，这些操作必须在机房里才可以进行，安装维护极为不便，为此我们需要安装VNC远程管理工具。

1. 安装配置VNC服务器

(1) 安装VNC服务器

```
# yum install tigervnc-server -y
```

(2) 修改VNC配置

VNC配置文件在/etc/systemd/system目录下，我们可以将/lib/systemd/system/vncserver@.service模板文件复制一份到该目录下并修改名称。

```
# cp /lib/systemd/system/vncserver@.service /etc/systemd/system/vncserver@:1.service
```

然后打开配置文件/etc/systemd/system/vncserver@:1.service替换掉默认用户名，找到下面这一行：

```
ExecStart=/sbin/runuser -l <USER> -c "/usr/bin/vncserver %i"
```

```
PIDFile=/home/<USER>/.vnc/%H%i.pid
```

这里需要用root账号登录，所以替换成：

```
ExecStart=/sbin/runuser -l root -c "/usr/bin/vncserver %i"
```

```
PIDFile=/root/.vnc/%H%i.pid
```

不建议使用普通账号登录VNC，因为容易产生各种

错误。

(3) 重新加载 systemd

```
# systemctl daemon-reload
```

(4) 设置 VNC 密码

```
# vncpasswd
```

确保输入的密码多于 6 个字符。

(5) 关闭和禁止防火墙

```
# systemctl stop firewalld.service
```

```
# 关闭防火墙
```

```
# systemctl disable firewalld.service
```

```
# 禁止开机启动防火墙
```

(6) 开启 VNC 服务

```
# systemctl enable vncserver@:1.service # 开机自动启动 VNC 服务
```

```
# systemctl start vncserver@:1.service # 启动 VNC 服务
```

(7) 使用客户端连接 VNC

现在, VNC 服务器的安装已经完成, 不过要连接到 VNC 服务器, 我们还需要在本地计算机上安装仅供连接远程计算机使用的 VNC 客户端。你可以用像 Tightvnc viewer 和 Realvnc viewer 此类的客户端来连接到 VNC 服务器 (如图 4)。



图 4 使用 VNC 客户端连接 KVM 服务器

如果需要更多的用户连接 VNC 服务器, 那就需要创建新的配置文件和端口。请返回到第二步, 添加一个

新的用户和端口。你需要创建类似 vncserver@:x.service 的配置文件, 并替换该文件里的用户名和之后步骤里相应的文件名、端口号, 并确保登录 VNC 服务器用的是之前配置 VNC 密码的那个用户名。

2. 其他常用命令

(1) 自动开启虚拟服务

```
# Systemctl enable libvirtd
```

(2) 查看虚拟机名称及状态

```
# virsh list --all
```

(3) 让虚拟机开机自动启动

```
# virsh autostart 虚拟机名称
```

设置完成后, 可以在 /etc/libvirt/qemu/autostart 下看到已设置自动启动的 KVM 配置文件链接。

经验总结

经过一段时间的运行, 证明虚拟化技术具备很多独特的优势, 网络管理和维护变得非常简单, 可以减轻网络管理人员的工作压力。对于很多基层单位来说, 网络服务虚拟化是一个不错的选择。

管理 Windows Server 2008 文件服务器

顾武雄

企业的不断成长，导致各种不同的网络资源越来越多越来越杂，因此，找到一项可以有效解决资源管理上的问题，成为了眼前最重要的工作之一。

文件服务器的技术发展到了 Windows Server 2008 版本，已经有了相当大的突破。因为在过去版本的应用中，许多功能的实现都是需要结合第三方产品才能够做到。然而，它所能发挥的功能还不仅于此，因为在高级文件安全管理中，它还能够借助 RMS 的服务器角色，来同时保护保存在文件服务器、Exchange Server 以及 SharePoint 文档库的文件安全，有效避免重要文件外流至企业以外的计算机中。

接下来，就让我们了解一下，Windows Server 2008 能够提供的基本网络资源管理特色有哪些。

分布式文件系统 (DFS)

这项功能主要解决了使用者没有单一入口去快速找到所需要的文件资源问题，以及提供重要多部文件服务器本地端或集成远程的复制机制，一方面解决文件服务器灾备问题，一方面则是解决移动工作者随时更改区域的联机存取问题。然而，这项功能早在 Windows Server 2000 版本就已经提供，不过在当时只能算是阳春版的 DFS 管理组件，如今 Windows Server 2008 版本中更是延伸了在 DFS 上的各项功能，例如对于带宽的配置、数据压缩的同步复制、报表分析以及全新直觉化的操作界面等。

文件服务器资源管理

以往对于文件服务器资源的管理机制不外乎就是共享权限的配置、磁盘配额的限制，而如今，Windows Server 2008 对于这一方面的管制措施已经可以管理到活页夹层级配额、存放文件的自动筛选、各类的警示通知

与报表分析等。

打印机集中配置

自行手动联机到每一部打印机服务器上去管理打印资源，只有在小型企业的 IT 环境中行得通，在中大型以上的企业管理中则必须要有一项集中配置的管理机制。而在 Windows Server 2008 的全新打印机管理界面中，可以达到集中配置与集成组策略的自动调配机制，彻底解决了长久以来 IT 在打印机集中管理上的难题。

如今，企业的 Active Directory 中都会有几部 Windows Server 2008 主机，如果您想让其中的服务器作为文件服务器，以提供全公司文件集中保存与管理，要如何进行设置与安装呢？

关于文件服务器功能的安装部分，首先我们必须先确认目前这部文件服务器可以在企业网络中被寻找到，以确定后续客户端计算机可以正常地进行联机存取。请在“控制台”中单击开启“网络和共享中心”，接着如图 1 所示展开“共享及探索”设置项目，将设置变更为“开启网络探索”，然后单击“应用”按钮即可。

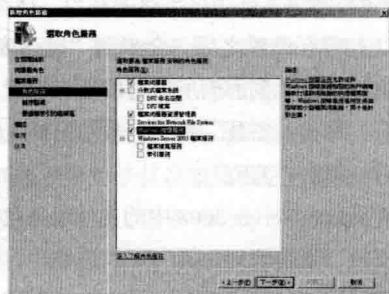


图 1 文件服务角色组件选取

完成以上设置后，我们便可以来安装 Windows Server 2008 文件服务器角色。在“开始→系统管理工具”下拉选单中，单击开启“服务器管理员”界面，在“角色”节点上单击“新增角色”，之后将会来到“选取服务器角色”页面。勾选“文件服务”，单击“下一步”。在

“文件服务”页面中,可以看到文件服务的简介,其中最重要的一项说明就是“在同一台计算机上不能同时安装 Windows 搜寻服务与索引服务”。单击“下一步”继续。

接下来,在“选取角色服务”页面中,便可以针对文件服务角色细项的组件进行选取安装,这里还包含了旧版 Windows Server 2003 文件服务的相关组件可以安装。在此,笔者先以分别勾选“文件服务器”、“文件服务器资源管理员”、“Windows 搜寻服务”三个组件来作为安装实例说明。单击“下一步”。

在“设置保存使用监视”页面中,勾选所要监视的磁盘。在默认状态下,只要使用量达到总容量的 85% 时,便会产生相关网页格式的分析报告,供系统管理员参考。

如果在上一步中不想直接应用系统默认值,可以单击“选项”按钮来开启“磁盘监视选项”页面,在此便可以设置磁盘使用量阈值,以及勾选当到达阈值时所要产生的报告项目。默认状态下,只会勾选“依拥有者列出的文件报告”、“依文件群组列出的文件报告”。

接下来在,“设置报告选项”页面中,需要设置报告文件保存的位置(默认值为 C:\StorageReports),以及是否要通过 SMTP 服务器发送 E-mail 报告给相关指定的使用者。在此强烈建议将公司内目前使用的 E-mail 服务器设置进来,并且通过分号的输入,让多位系统管理人员都可以收到这些分析报告。

在前面文件服务角色组件的安装中,如果勾选了“Windows 搜寻服务”,那么将会出现“为 Windows 搜寻服务选取要编制索引的磁盘区”页面,您可以将所要编制索引的磁盘区勾选,以利于后续客户端可以通过 Windows 桌面搜寻功能,来快速在这部文件服务器上找到他们需要的文件。

完成以上所有设置之后,会来到“确认安装选项”页面。在此,可以看到前面所做过的所有设置属性,确认无误之后,单击“安装”按钮。成功完成文件服务角色安装之后,单击“关闭”。

完成 Windows Server 2008 中的文件服务角色安装之后,便可以从“系统管理工具”下拉选单中,开启“文件服务器资源管理员”界面,来做进一步的配置。接下来介绍的每一项设置,都可以根据实际需求进行选择。

如图 2 所示的是开启后的“文件服务器资源管理员”界面,通过这个界面,可以让系统管理员进行有关保存配额的管理、文件检测的管理以及存放设备报告的管理等。在此我们先在最上层的项目节点上,单击位于动作窗格中的“设置选项”,来看看有哪些基本的配置需要

完成。

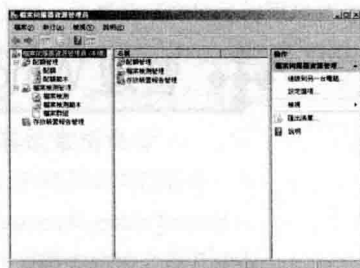


图 2 文件服务器资源管理员

首先,在“电子邮件通知”页面中,所有文件服务器管理中的警告通知都必须先完成这部分的设置,在此必须指定发信的 SMTP 服务器以及默认收信的管理 E-mail。对于发件人的 E-mail,建议采用默认值即可。设置完成后,单击“传送测试电子邮件”按钮,试试看能不能收到一封测试信件。在“通知限制”页面中,主要用于避免发生在短时间内,让系统管理员收到重复的相关通知,因此,可以在此针对不同的通知方式来设置通知限制的时间,包括电子邮件通知、事件日志通知、命令通知以及报告通知。

在“存放设备报告”页面中,可以预先设置好后续报告中每个项目所要报告的信息参数,例如,单击“大型文件→编辑参数”按钮来设置认定的大型文件的大小标准值,或是自定义“最近未存取过的文件”所要定义的天数(默认值为 90 天)等。针对“大型文件”的报告项目,开启“报告参数”页面,在默认状态下文件大小下限值为 5MB。此外,还可以在下方字段中设置惟一所要应用的文件类型。

在“报告位置”页面中,主要是设置各种不同报告类型的保存路径,分别说明如下:

● 随附报告活页夹

当使用者超过后续所定义的保存配额大小时,以及发生尝试存取没有权限的文件时,这些报告文件的保存路径。

● 日程报告活页夹

存放所有根据日程设置所产生的报告文件。

● 依需求报告活页夹

管理者自行手动产生的立即报告文件。

最后,在“文件检测审核”页面中,如果您希望系统能够审核所有文件检测的活动,可以勾选“在审核数据库中记录文件检测活动”选项,后续在报告中便可以看到这部分的审核报告信息。单击“确定”按钮完成以上所有页面组态的设置。

Windows Server 2008 版本中提供的配额管理机制,已经不再是过去只能针对磁盘区来进行设置而已,而是与 Windows Server 2003 R2 版本一样,能够直接对特定的本地活页夹或共享文档夹进行设置,并且可以自动以 E-mail 的警告来分别通知管理者与相对应的使用者,管理者还可以进一步产生所需要的报表,来方便后续在保存配额政策上的管理与追踪。

要想新增一个配额设置,要先单击至“配额管理→配额”项目节点上,单击位于“动作”窗口中的“建立配额”继续。在表 1 中,对新版配额管理功能进行了比较。

表 1 新旧版配额管理功能比较

配额特色	文件服务器资源管理员	NTFS 磁盘配额
配额追踪	可针对活页夹或磁盘	只能针对磁盘来配额
磁盘量使用计算	实体的磁盘空间	逻辑的文件大小
通告机制	可透过 E-mail、自定义的报告、外部命令的执行以及事件查看器的记录	惟一事件查看器的记录

在“建立配额”页面中,可以选择是否要让配额设置自动应用在后续所建立的子活页夹上,否则该配额设置只会针对单一层的活页夹总容量进行配额使用量监测。接着,在配额属性设置中,可以直接选择所要应用的配额模板,或是自定义配额属性。在此,我们选取“定义自定义配额属性”,单击“自定义属性”继续。紧接着可以选择所要复制的配额模板项目,然后再来修改空间限制的值,并且决定是要采用强制限制的固定配额方式,还是采用纯粹用于监视的弹性配额方式。接着,单击“新增”按钮来设置“通知阈值”。

在“新增阈值”页面,可以针对此新增的配额设置,加入四种不同的阈值到达时所要执行的操作,分别有电子邮件信息、事件日志、命令以及报告。首先以“事件日志”设置为例,设置当配额设置达到阈值时所要产生的事件记录属性,您可以不作任何修改直接采用默认值,或是加入自己希望显示的变量,每一个变量的选择,在下方都会有相对的中文说明。

关于“报告”页面的设置,首先勾选所要产生的报告项目,并且可以设置产生的报告是否要一并传送给指定的系统管理员 E-mail,以及传送给超过阈值的使用者。在此建议至少将后者的设置勾选。

若想要将各种配额设置到不同的活页夹中,也可以先建立好自定义的配额模板,展开“配额管理”节点,在“配额模板”项目上点击鼠标右键,选择“建立配额模板”,或是直接在“动作”窗口中单击“建立配额模板”。

接下来便可以开始输入模板名称(例如:依照部门、活页夹类型等方式)、空间限制大小值、发送通知的临界值。在通知部分会至少定义一个默认的限制(100%),以及一个警告层级的临界值(85%),也可以在额外新增定义更低的临界通知值。此外,在配额管理上也可以选择固定配额或弹性配额,后者主要用来监视与了解使用者的存取状况,在超过额度时并不会强制禁止使用者的存取。最后,建议在每一个配额的限制值中设置使用者与管理员的 E-mail 通知,而警告层的通知只给使用者知道就可以了。

无论配额大小的设置如何,只要在报告设置中勾选了产生事件日志的设置,那么只要有使用者所存放的文件超过了所设置的阈值,在事件查看器的“应用程序”类别中,便可以看到事件标识符为 12325 的警告事件项目,其属性将会清楚说明因哪一位使用者的存取造成此事件的产生,以及所设置的配额大小与目前所使用的保存空间大小。

在 Windows Server 2008 的文件服务器管理机制中,除了可以限制使用者的保存配额之外,是否有这样的管理功能,可以用来限制保存的文件类型,以便让不同活页夹的文件保存,能够惟一保存属于它所保存的文件?

的确,除了对活页夹进行配额的管理之外,管理人员还可以进一步针对这些活页夹设置文件检测机制,也就是对于使用者所能够放置的文件类型进行管制。在“文件检测管理”节点项目上,展开至“文件检测”项,点击鼠标右键,选择“建立文件检测”,或是直接在“动作”窗口中单击“建立文件检测”。接着,设置所要设置的文件检测路径,以及选择适当的现有检测模板,或是单击“自定义属性”来额外定义。关于检测模板与文件群组的定义,管理员也同样可以预先自行新增设置。

如图 3 所示便是我们所成功新增的一笔文件检测设置,后续如果需要对于其设置属性进行修改时,则只要在选取此项目时再单击位于“动作”窗口中的“编辑文件检测属性”即可。完成了文件检测设置之后,便可以开始将被封锁的文件类型复制到此活页夹,系统将会立即弹出一个警示信息,从信息属性看来,您可能会觉得好像是权限设置造成的问题,然而实际上是被文件检测的封锁功能应用所致。

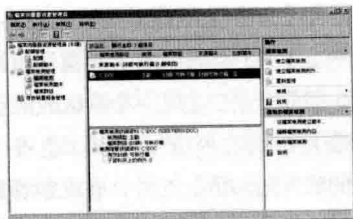


图3 完成文件检测新增

同样的，只要在文件检测设置报告中有勾选事件日志的通知，那一旦发生了违反保存限制的事件时，打开事件查看器，便可以在“应用程序”类别中，看到有关事件标识符为 8215 的警告事件，其属性中说明了产生此事件的原因，包括尝试保存这些文件的使用者是谁，以及所要存放的文件名称是什么等。

如同配额管理的模板一样，我们也可以在“文件检测模板”的节点项目上，来查看系统默认的模板有哪些，以及单击位于“动作”窗口中的“建立文件检测模板”，来建立自定义的检测模板，以供后续新增的文件检测设置来直接应用。

在检测模板的新增中，必须设置所要应用的文件群组类型。在系统默认状态下，已经帮我们建立好了许多常见的文件群组类型项目，在此针对特定的文件群组进行编辑修改，或者是建立自定义的文件群组即可。我们以编辑现有默认的 Office 文件群组为例，由于笔者发现在这个文件群组的列表属性中并没有包括 Office 2007 的副文件，因此自行加入像 *.docx、.pptx 等扩展名清单，必要时，也可以新增所要排除的文件格式清单。

在 Windows Server 2008 的文件服务器管理中，系统管理员如何掌握整个文件服务器运行状态，以及随时了解到使用者对于资源的存取情形呢？

其实，在文件服务器资源管理功能当中，可以直接针对文件服务器的存取状况产生存取状况分析报告，这样便可以有效掌握各种不同类型的文件存放情况。执行的方法很简单，只要在“存放设备报告管理”的节点上

点击鼠标右键，或是直接单击位于“动作”窗口中的“计划新的工作报告”或是“立即产生报告”。在此，笔者以执行立即产生报告作为示例，单击“新增”按钮，选择所要产生存放报告的活页夹路径，接着便可以在下方勾选所要产生报告的数据类型，如：大型文件、重复文件、配额使用量报告等。至于呈现的报告格式，可以选择 DHTML、HTML、XML 等样式。

完成立即产生报告的属性设置之后，单击“确定”，将会出现“产生存放设备报告”对话框，在此您可以决定是要“等到产生报告后再显示这些报告”，还是要“在背景产生报告”。如果在前面的操作步骤中您单击了“计划新的报告工作”，除了同样可以设置有关报告的活页夹与报告类别之外，其中报告传递的 E-mail 地址输入是不可少的，至于多出来的“计划”页面中的设置，当然也会是必要的设置之一。

在默认状态下，有关计划报告的设置是空白的，我们必须在此页面中进行新增。在此笔者新增一份报告计划设置，并且单击“编辑计划”来查看与修改原有的属性设置。在“计划”页面中，可以设置工作计划的类型（例如：每天、每周、每月等）、开始时间等设置，必要时还可以单击“进阶”按钮，来设置更进一步的计划定义。

在“进阶计划选项”的设置页面中，除了可以设置开始日期外，还可以设置结束的日期，以及重复执行的时间间隔。当新增了一份计划报告作业后，往后仍然可以继续新增其他不同定义的计划报告设置，或是针对指定的计划作业报告项目进行编辑或删除等。

无论您在前面的操作中是选择立即还是计划任务的方式来产生报告，只要有勾选的报告类型，都会在执行不久产生与自动开启指定的报告属性。例如，您可以开启一个大型文件的报告，或是开启一个文件检测审核报告的范例。

❖ 初始化已使用的硬盘

▼ 河北 王春海

在配置 VSAN 的时候，我们知道，组成 VSAN 服务器中的本地硬盘，应该是未使用的。如果你的硬盘已经使用过，需要使用工具删除原来硬盘上所有分区，才能被 VSAN 分配使用。如果你配置了 VSAN 之后，在 VSAN 中“看”不到硬盘或硬盘数量不对，则表示硬盘未被初始化。在新的 VSAN 6.2 中，在 vSphere Web Client 中，可以初始化这些硬盘。下面通过具体的案例进行介绍。

1. 在一个 VSAN 群集中，172.18.96.44 的主机有 1 个 120GB 的 SSD、2 个 1TB 的 HDD，系统装在一个 2GB 的 U 盘中。

2. 但是在“VSAN → 管理 → 设置 → 磁盘管理”，172.18.96.44 只识别出一块 1TB 的硬盘示。

3. 选中 172.18.96.44，在“管理 → 存储器 → 存储设备”选项中，先选中一个 1TB 的硬盘，单击“全部操作”，

在下拉菜单中选择“清除分区”。

4. 在“您即将永久删除该设备上的所有现有分区”对话框中，显示了当前分区的信息。如果显示“VSAN 元数据”，表示这是被 VSAN 正确识别并使用的磁盘，单击“取消”按钮，取消本此操作。

5. 再次返回“存储设备”列表，选择另一个磁盘，选择“清除分区”，如果显示了不同的分区信息，例如本次显示“HPFS/NTFS”信息，表示这个磁盘以前是由 Windows 使用的，单击“确定”按钮，清除该设备上的所有现有分区。

6. 返回到“VSAN”磁盘管理界面，可以看到 172.18.96.44 的磁盘组，已经正确识别了这块磁盘。如果你的 VSAN 是“手动”模式，你需要手动向磁盘组中添加这块磁盘，这些基本操作就不再介绍。

❖ 用组策略修改主页设置

▼ 河北 王春海

由于用户的使用习惯，仍有部分用户选择继续使用 Windows XP 系统。而 IE 浏览器的版本也在不断升级，在 Windows XP 系统下从 IE 6 升级到 IE 7 及以上版本时，就会出现一个问题：打开浏览器后，不会自动跳转到自己设置的主页，而是会跳转到 Microsoft 主页。

IE7 主页不管用，修改组策略

每次打开 IE 浏览器，都先打开 Microsoft 主页，虽

说不是什么大问题，但是对于使用者来说也会有一些不方便。如何解决这个问题？对组策略编辑器里的 IE 选项进行设置即可。

1. 单击“开始 → 运行”，输入“gpedit.msc”，打开“组策略编辑器”。

2. 打开“组策略编辑器 → 计算机配置 → 管理模版 → Windows Components → Internet Explore”（如图 1 所示）。

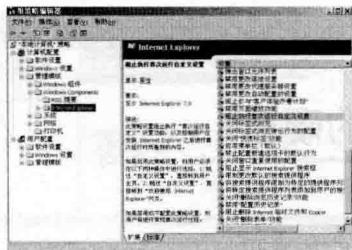


图1 组策略编辑器

3. 在“组策略编辑器”窗口页面右边栏找到“阻止执行首次运行自定义设置”这一项，双击打开此项属性设置，选择“已启用”，选择您的选择选“直接转到主页”就可以了（如图2所示）。

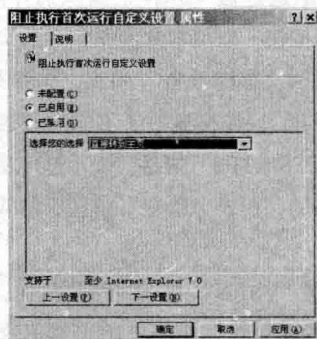


图2 阻止执行首次运行自定义设置

4. 打开 IE 浏览器，重新设置你的主页，单击“应用”按钮。重启 IE，这时，浏览器会直接打开你设置的主页了。

注意

修改组策略后，一定要重新设置一次主页，否则不会起作用。

没有 IE 这一项怎么办

笔者在解决这类问题的时候还发现，有时候打开的组策略编辑器里并没有 Windows Components 这一项，那它下面的 Internet Explorer 就看不到了，这通常见于 Windows XP 升级到 SP3 版本后，或是 Windows Server 2003 及 Windows XP 系统的不同版本导致组策略编辑器里的选项不全。解决方法如下。

1. 打开“组策略编辑器→计算机配置→管理模板”，在“管理模板”上单击右键，选择“添加/删除模板”（如图3所示）。

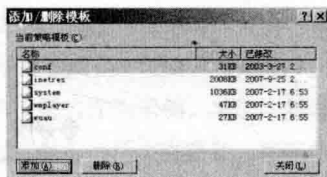


图3 添加策略模板

2. 在弹出的窗口点击“添加”，选择“inetres.adm”文件，返回关闭模板窗口，就看到选项出来了（如图4所示）。



图4 选择模板文件

模板文件是什么

组策略修改的其实就是注册表。Windows 的注册表保存了系统关键的数据信息，随意更改可能会出现错误，严重的甚至会引起系统崩溃。而组策略就提供了安全、高效的修改注册表的一种方式。组策略一共有两种，计算机策略和用户策略。目前，通过管理模板可对 1300 多种不同的注册表设置进行修改，包括从配置网络设置到禁闭用户桌面等系统选项的设置。

其中，Windows 默认安装了一些模板，其名称和作用分别是：

System.adm：显示配置核心 OS GUI 特征的策略设置，即系统策略设置。

Inetres.adm：显示配置 Internet Explorer 的策略设置。

Wmplayer：显示配置 WindowsMediaPlayer 的策略设置。

Conf.adm：显示配置 NetMeeting 的策略设置。

Wuau.adm：显示配置自动更新的策略设置。

需要注意的是，操作系统的版本不同，缺省安装的管理模板也不一样。除上述这些管理模板外，还有其他标准管理模板。

Inetcorp.adm：显示配置拨号上网、语言和 Internet Explorer 临时文件的策略设置。

Inetset.adm：显示配置 Internet Explorer 的其他策略

设置。

除以上标准模板外,也可下载其他模板,甚至可以

创建自己的模板。有时候组策略某项缺失,只需找到对应的模板文件添加上即可。



用 Linux 巧解硬盘逻辑锁

福建泉州 李贵华 曾玮琳 梁国均

硬盘逻辑锁指的是安装 Windows 系统的计算机在使用 MS-DOS 引导启动时,会搜索所有正常挂载的逻辑盘,并且按顺序分配合适的盘符以供系统调用。此过程以硬盘主引导扇区的分区表信息为准,如果主引导分区记录被修改,所有逻辑分区起始位置指针始终指向第一个逻辑分区,使得系统启动在查找逻辑分区时形成死循环,不能完成遍历逻辑分区的任务,造成硬盘长期读写,系统不能启动。

硬盘逻辑锁往往是因恶意软件、计算机病毒、非正常关机等引发,会导致计算机已安装的 Windows 操作系统启动时提示找不到有效启动分区,或者启动进度条“死循环”,不能继续启动,但硬盘数据指示灯常亮。硬盘逻辑锁发生后,进入 BIOS 设置查看硬盘信息均正常,模式设置也正确。使用 Windows 系统安装盘或 Windows PE 系统启动电脑也会失败。如果把故障硬盘连接至其他正常计算机作为从盘挂载,也会导致该计算机启动失败。

常见的解决硬盘逻辑锁方法包括热插拔硬盘、利用修改版 MS-DOS 引导盘启动、绕过 BIOS 修改硬盘参数等,但这些方法操作难度大,成功率低,且存在硬件损坏、数据丢失的较大风险。由于硬盘逻辑锁的实质是 MS-DOS 系统在启动时的小缺陷,因此,可以利用无需 MS-DOS 引导启动的操作系统(如 Linux 操作系统),避开硬盘逻辑锁启动计算机,重建硬盘分区表信息,再利用 PE 工具恢复硬盘分区和数据,从而解决硬盘逻辑锁故障。这种解决方法具有操作性强、可靠性高的特点。

制作启动盘

目前 Linux 发行版本较多,特色各异。建议选择体积小、功能齐全的 Linux 发行版本,如 Puppy Linux、

CD Linux 等。这类 Linux 发行版本具有图形化中文界面、操作方便、自带软件丰富、网络功能强。下载好 Linux 发行版本的镜像文件后,利用 UltraISO 软件将其制作成可启动光盘或可启动 U 盘。

启动计算机

开启故障计算机,进入 BIOS 设置,视情况将第一启动项设置为光驱或 USB 设备。保存 BIOS 设置,放入光盘或插入 U 盘,重新启动故障计算机,使其加载 Linux 系统,进入 Linux 系统桌面环境。

修复硬盘主引导记录

点击桌面“驱动器”,查看 /dev/sda/ 目录下硬盘是否正常挂载,然后运行系统集成的 GParted 硬盘管理软件,选择“设备→创建分区表”选项,重建分区表信息。随后运行 TestDisk 软件修复磁盘分区,成功后则可以利用 Windows PE 重新启动电脑。

恢复硬盘数据

使用 Windows PE 系统启动计算机,运行 DiskGenius 软件,点击搜索分区,范围选择“整个硬盘”,搜索过程中提示有搜索到的分区,则选择“保留”,直到所有分区搜索完毕。点击“保存更改”,则硬盘的分区信息得到恢复,且硬盘数据能够恢复。如有部分数据异常,可继续利用数据恢复软件进行恢复,这类软件较多,在此不再赘述。

至此,借用 Linux 操作系统解开了硬盘逻辑锁,同时硬盘上的数据没有丢失,完美解决硬盘逻辑锁问题。

让虚拟机实现互动

河北 王春海

vSphere 是 VMware 用于企业数据中心的虚拟化产品，Workstation 是 VMware 面向 IT Pro、工程师及个人的虚拟机产品，网管人员经常使用 VMware Workstation 测试虚拟机，有时需要将 Workstation 配置或测试好的虚拟机上载到 ESXi。而有的时候，管理员需要将 vSphere 中的虚拟机“下载”到 Workstation 使用，这就涉及到不同平台之间“虚拟机”的“复制”问题。本文介绍 VMware Workstation 与 vSphere 之间“交互”虚拟机的方法。

Workstation 连接到 vSphere 直接上传下载

在高版本的 VMware Workstation 中，可以直接连接到 vSphere (VMware ESXi 或 vCenter Server)，并且可以将虚拟机从 Workstation 上传到 vSphere (VMware ESXi 或 vCenter Server)，或者将虚拟机从 vSphere 下载到 Workstation。无论是上传还是下载，虚拟机在源位置都保留不变，所以这不是“迁移”，而是“复制”。

上传虚拟机

使用上传功能，可以满足大多数的需求，但是需要注意，将虚拟机从 Workstation 上传到 vSphere 后，虚拟硬盘会变为“厚置备”磁盘，而从 vSphere 下载虚拟机到 Workstation，则是“精简置备”。使用 Workstation 连接 vSphere 上传虚拟机的主要步骤如下。

1. 打开 VMware Workstation 控制台，在“文件”菜单中选择“连接服务器”，在弹出的“连接服务器”对话框中，在“服务器名称”处输入要连接的 VMware ESXi 或 vCenter Server 的 IP 地址，之后输入要连接的服务器的管理员账户及密码，单击“连接”按钮连接（如图 1 所示）。



图 1 连接服务器

2. 在弹出的“无效的安全证书”对话框中，单击选中“总是信任具有此证书的主机”，然后单击“仍然连接”按钮。在弹出的“VMware Workstation”对话框中，选中“不再显示此消息”，然后单击“记住”按钮，记住当前的登录信息及密码。

3. 如果要将虚拟机从 Workstation 上传到刚才连接的 vSphere，则在 Workstation 中，按 F9 热键，打开左侧的“库”列表，在库列表中选择要上传的虚拟机（注意，需要提前将虚拟机关闭电源，并修改该虚拟机的光驱、软驱，使之先不要加载镜像），用鼠标右键单击，在弹出的快捷菜单中选择“管理→上传”（如图 2 所示）。



图 2 上传

4. 在弹出的“上传虚拟机向导”对话框中，在“目标服务器”中选择要放置虚拟机的服务器，在此可以在列表中选择第一步连接的 vSphere。在“选择目标位置”对话框，在“主机”列表中选择要保存虚拟机的虚拟机，

并在“数据存储”中选择将虚拟机保存在哪个存储,在“名称”处设置上传后虚拟机的名称,然后单击“完成”按钮,之后开始上传。

5. 上传完成后,使用 vSphere Client 登录到 vSphere,选中上传后的虚拟机,单击“编辑虚拟机设置”。在“虚拟机属性”对话框中,可以根据需要,修改上传后虚拟机的内存与 CPU 大小。在“硬盘 1”中可以看到,上传后的虚拟硬盘属性为“厚置备延迟置零”。



图 4 下载后硬盘是精简置备

下载虚拟机

如果要下载虚拟机从 vSphere 下载到 Workstation,则可以使用如下的操作,步骤如下。

使用 Workstation 连接到 vSphere,连接之后,按 F9 显示库,在库中选中连接的 vSphere,在左侧清单中选择要下载的虚拟机,用鼠标右键单击,在弹出的快捷菜单中选择“管理→下载”(如图 3 所示)。在“下载虚拟机”对话框中,为下载虚拟机设置名称及本地保存位置,然后单击“下载”按钮开始下载虚拟机。



图 3 下载

下载之后即可以在 Workstation 中修改虚拟机配置、启动虚拟机。另外,如果打开“资源管理器”,查看下载后的虚拟机,可以看到,下载后的虚拟机硬盘是“精简置备”。在 Workstation 中编辑下载后虚拟机的设置,在图中可以看到,虚拟硬盘最大是 40GB,当前大小是 5.4GB,这也可以看到磁盘属于“精简置备”(如图 4 所示)。

在 Workstation 与 vSphere 中使用 OVF 文件交互

可以在 Workstation 或 vSphere 中,将虚拟机导出成 OVF 文件,然后在 vSphere 或 Workstation 通过“导入 OVF 文件”的方式,进行虚拟机的交互。在使用 OVF 文件在 Workstation 与 vSphere 之间交互时,要注意 Workstation 虚拟机及 vSphere 产品的版本。

例如,在 VMware Workstation 12 中创建的虚拟机,默认是 12.0 的硬件格式,则在 Workstation 中导出的 OVF,不能导入 ESXi (因为当前 ESXi 最高版本是 6.0,最高只能支持到 11 的硬件版本)。如果要将 Workstation 12 的虚拟机,导入到 vSphere 6 中,则在导出 OVF 文件之前,需要先修改硬件版本到 11 才可。同样,ESXi 6 中创建的虚拟机,如果虚拟机硬件版本为 11,则至少需要导入到 Workstation 11 中才可以,不能导入到 Workstation 10 中。但如果在 ESXi 6 中创建虚拟机时,采用的虚拟机硬件版本 9,则可以导入到 Workstation 9 及其以下的 Workstation 版本中。在 ESXi 中,虚拟机一旦创建,其虚拟机的硬件版本只能“升级”不能下降,而在 Workstation 中,可以通过“更改硬件兼容性”,升级或下降虚拟机的硬件版本。

虚拟机硬件版本与 Workstation、ESXi 版本对应关系如表 1 所示。

表 1 虚拟机硬件版本与及其支持的最低 Workstation 与 ESXi 版本对应表

虚拟机硬件版本	最低 Workstation 版本	最低 ESXi 版本
12	12	
11	11	6.0
10	10	5.5
9	9	5.1
8	8	5.0

在 vSphere 中导出 OVF

在 vSphere 中将虚拟机导出为 OVF 的主要步骤如下。

1. 使用 vSphere Client (vSphere Web Client 也可, 本文以 vSphere Client 为例) 连接到 ESXi 或 vCenter Server, 关闭准备导出为 OVF 文件的虚拟机, 然后修改虚拟机设置, 修改“CD、DVD 驱动器”为“客户端设备”(如图 5 所示)。



图 5 修改虚拟机设置

2. 在左侧清单中选择一个关闭电源的虚拟机, 在“文件”菜单选择“导出→导出 OVF 模板”(如图 6 所示)。



图 6 导出 OVF 模板

3. 在“导出 OVF 模板”对话框, 设置导出的名称、选择导出的目录, 在“格式”列表中选择是导出文件夹 (OVF) 还是单个文件 (OVA), 之后开始导出 OVF 模板, 直到导出完成。导出完成后, 将导出的文件 (文件夹) 通过网络或活动硬盘复制到 Workstation 或其他 vSphere 虚拟机处备用。

在 vSphere 中部署 OVF 模板

当使用 vSphere Client 直接连接到主机时, 可以通过 vSphere Client 计算机可访问的本地文件系统或通过 Web URL 部署 OVF 模板。

1. 使用 vSphere Client 登录到 vCenter Server, 在“文件”菜单选择“部署 OVF 模板”。在“源”对话框中, 单击“浏览”按钮选择 OVF 或 OVA 模板。在“OVF 模板详细信息”对话框, 显示了要部署的模板虚拟机, 占用的磁盘空间 (精简磁盘占用空间和厚置备磁盘占用空

间)。

2. 在“名称和位置”对话框, 为已部署模板指定名称和位置。在“主机/群集”, 选择要在哪个主机或群集上运行部署的模板。在“资源池”对话框, 选择要在其中部署模板的资源池。在“存储器”对话框, 选择将虚拟机文件存储在何处, 你可以根据需要选择。在“磁盘格式”对话框, 选择以何种格式存储虚拟磁盘, 一般选择“精简置备”。在“网络映射”对话框, 选择已部署的虚拟机使用什么网络。在“即将完成”对话框, 显示了部署信息, 检查无误后单击“完成”按钮。

之后开始部署虚拟机, 直到部署完成。部署之后, 虚拟机出现在清单中 (如图 7 所示)。



图 7 从模板部署虚拟机

在 Workstation 中更改虚拟机硬件版本

在 Workstation 中可以更改虚拟机的硬件版本, 以适应其他版本的 Workstation 或 vSphere。

1. 在 Workstation 中, 用鼠标右键单击要更改的虚拟机 (虚拟机要关闭电源), 在弹出的快捷菜单中选择“管理→更改硬件兼容性”(如图 8 所示)。

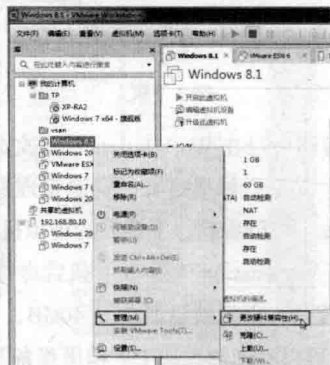


图 8 更改硬件兼容性

2. 在“选择虚拟机硬件兼容性”对话框中, 在“硬件兼容性”列表中, 选择新的硬件版本, 在“兼容产品”处会显示当前选中版本所支持的 vSphere 版本。在“转换前克隆”对话框, 选择“更改此虚拟机”。

3. 在“查看更改”对话框,显示应用的更改,单击“完成”按钮。之后会开始转换虚拟机并完成虚拟机硬件的更改。

在 Workstation 中导出与导入 OVF

在 Workstation 中导出与导入 OVF, 与在 vSphere 中类似, 但比在 vSphere 中更简单。

1. 在 Workstation 中,选中导出为 OVF 的虚拟机(虚拟机要关闭电源), 然后在“文件”菜单中选择“导出为 OVF”。

2. 在弹出的“将虚拟机导出为 OVF”对话框中, 选择保存 OVF 文件的位置, 单击“保存”按钮, 之后 Workstation 将会导出该虚拟机。

如果要在 Workstation 中导入 OVF, 可在 Workstation 中,从“文件”菜单选择打开“按钮”。在“打开”对话框中,浏览选择要导入的 OVF 文件。在“导入虚拟机”对话框中,设置导入的虚拟机名称及保存位置,单击“导入”按钮(如图 9 所示), 之后则完成虚拟机的导入。

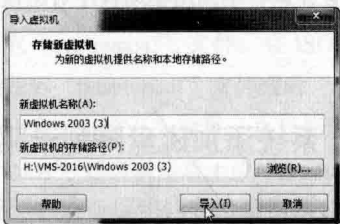


图 9 导入虚拟机

存储浏览器复制或下载

如果在两个 vSphere 之间互相传送虚拟机, 而这 vSphere 又没有在同一个网络中, 除了使用导出、导入 OVF 的方法外, 还可以使用 vSphere Client 或 vSphere Web Client, 通过下载、上传虚拟机文件夹的方式交互。

从 vSphere 下载虚拟机

可以通过浏览 ESXi 的存储, 下载虚拟机所在文件夹的方式, 将虚拟机下载到本地, 保存在活动硬盘, 然后将此活动硬盘拿到另一个 vSphere 处, 使用“上载文件夹”的方式, 传送虚拟机。在 vSphere 中下载虚拟机文件夹的方法如下。

1. 使用 vSphere Client 登录到 vCenter Server 或

ESXi, 在左侧选中 ESXi 主机, 在“配置→存储器”中, 右击浏览保存虚拟机的存储器, 选择“浏览数据存储”(如图 10 所示)。



图 10 浏览数据存储

2. 在“数据存储浏览器”中, 在右侧选择要下载的虚拟机文件夹(不要展开该虚拟机), 单击工具栏上的“”按钮, 将此虚拟机下载到本地计算机(如图 11 所示)。

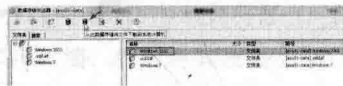


图 11 下载文件夹

3. 在“浏览文件夹”对话框中, 选中一个位置, 保存要下载的文件夹, 之后 vSphere Client 将下载选定的文件(夹)。下载之后, 打开“资源管理器”, 可以看到, 下载的虚拟硬盘是“厚置备”格式。

如果要在 Workstation 中使用此虚拟机, 则在 Workstation 的“文件”菜单中选择“打开”命令, 浏览选择下载后的虚拟机的配置文件(vmx 文件)即可打开。

将虚拟机上传到 vSphere

将虚拟机文件夹从 vSphere 下载到本地之后, 可以通过网络、活动硬盘复制到另一个 vSphere 中, 然后将虚拟机文件夹上传到 ESXi 存储, 同将虚拟机添加到 ESXi 清单的方式, 完成不同 ESXi 之间的交互。

1. 使用 vSphere Client 登录到 vCenter Server 或 ESXi, 在左侧选中 ESXi 主机, 在“配置→存储器”中, 右击浏览保存虚拟机的存储器, 在弹出的快捷菜单中选择“浏览数据存储”。

2. 在“数据存储浏览器”对话框中, 左侧选择根(/)路径, 单击“”按钮, 在弹出的下拉菜单中选择“上传文件夹”。

3. 在“浏览文件夹”对话框中, 浏览本地将要上传的虚拟机文件夹, 之后开始上传。上传完成后, 在“数据存储浏览器”中, 展开上传后的文件夹, 用鼠标右键单击.vmx 文件, 在弹出的快捷菜单中选择“添加到清单”。在“添加到清单”对话框中, 为新添加的虚拟机命名,

可以选择默认名称。之后根据向导完成虚拟机的添加。

4. 如果要在新的 ESXi 中启动虚拟机, 因为虚拟机是从另一个 vSphere 中“移植”过来的, 第一次不能启动, 此时虚拟机前面出现“气泡”标示, 单击“摘要”选项卡, 在“虚拟机消息”中, 选择“I Moved It”或“I Copied it”, 然后单击“确定”按钮(如图 12 所示)。之后虚拟机即可正常启动。

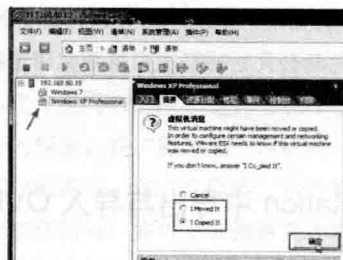


图 12 复制或移动虚拟机

向 WinPE 添加服务器驱动

福建泉州 李贵华

大多数系统维护员对于 WinPE 系统应该都不会陌生的, WinPE 系统即是 Windows 预安装环境(Windows Preinstallation Environment, 简称 WinPE)在 Windows 内核上构建的具有有限服务的最小 Win32 子系统, 它用于向准备安装 Windows 操作系统的计算机提供安装环境, 启动 Windows 安装程序, 复制文件或者制作磁盘映像, 是计算机技术保障人员日常工作中的有效工具。

目前, 随着单位服务器的维护工作量日益增多, 尽管使用最新内核的各种 WinPE 系统能将大多数服务器的磁盘阵列卡驱动都包含其中, 也不排除有个别的服务器, 由于 WinPE 系统中缺少服务器特殊阵列卡所需的驱动程序, 从而无法使用。实际上, 我们按照下面的方法, 可以将维护服务器所需的各类驱动程序添加进 WinPE 中, 制作出针对某种型号服务器的 WinPE 系统来帮助我们做好维护工作。下面, 笔者以添加服务器的磁盘阵列卡驱动为例和大家一同探讨。

系统进入驱动程序所在的子目录, 将驱动程序拷贝到指定的安装目录下面。完成驱动程序的拷贝操作之后, WinPE 系统会在运行中调用驱动程序对磁盘阵列卡进行驱动。

向 WinPE 系统添加磁盘阵列卡驱动程序

对 WinPE 调用磁盘阵列卡驱动程序流程有一定的了解后, 我们就可以逆向把磁盘阵列卡驱动程序添加到 WinPE 中了。首先, 用专用软件将 WinPE 系统的核心文件从压缩的镜像文件中提取出来, 然后把磁盘阵列卡驱动程序添加到这个提取出来的文件中, 再修改系统安装信息文件, 确保 WinPE 系统能够正确调用新添加的驱动程序。最后, 将修改后的文件封装压缩, 替换原先的文件, 完成 WinPE 系统的制作。具体步骤如下。

WinPE 系统制作

1. 提取 WinPE 系统镜像文件

首先使用 ULTRAIISO 或其他光盘映像文件制作编辑软件, 将 WinPE 系统镜像文件中扩展名为“IS_”的文件提取出来, 将这个扩展名改为“cab”, 然后用 WinRAR 或其他解压缩软件将其解压缩, 得到相应的 ISO 镜像文件。

WinPE 调用磁盘阵列卡驱动程序的流程

在制作专用 WinPE 系统之前, 首先要对 WinPE 调用磁盘阵列卡驱动程序的过程有一些简单的了解。计算机启动之后, WinPE 系统首先会读取磁盘阵列卡里面的硬件标识, 完成对磁盘阵列卡的识别工作。接下来, WinPE 系统会根据系统安装信息文件的信息, 通过磁盘阵列卡的标识找到对应驱动程序的名称, 然后 WinPE

2. 添加磁盘阵列卡驱动

在获得 ISO 镜像之后,接下来的工作是将磁盘阵列卡驱动程序添加到 ISO 镜像的相应位置。首先查出磁盘阵列卡的型号以及 WinPE 系统的内核版本,然后找出与磁盘阵列卡以及 WinPE 系统相匹配的驱动程序。在文件夹中,服务器阵列卡的驱动程序扩展名为“SYS”,用 WinCAB 软件将其打包,生成对应的 CAB 文件,然后,将该文件的扩展名改为“SY_”。最后,将该文件通过 ULTRAISO 添加到 ISO 镜像文件中存放驱动程序的位置中,通常位于文件夹“\SYSTEM32\DRIVERS”中,不同的 WinPE 系统可能会有差异。

3. 修改系统安装信息文件

将服务器磁盘阵列卡驱动程序添加到 ISO 镜像文件之后,还需要修改系统相应的安装信息文件,使得 WinPE 系统能够正确读取并安装该驱动程序。因此,我们需要对系统的“txtsetup.sif”文件进行配置,“txtsetup.sif”是 WinPE 系统在安装时加载驱动程序的信息文件,且该文件不在系统保护文件的范畴内,这意味着我们可以对这个文件任意修改而不用担心遭到操作系统的阻止。

(1) 获取“txtsetup.sif”文件。在 ISO 镜像文件里面可以直接找到“txtsetup.sif”文件或者“txtsetup.SY_”文件。对于“txtsetup.SY_”文件,将其提取出来,后缀名修改为“CAB”,然后解压缩生成“txtsetup.sif”文件,可以通过 ULTRAEDIT 或者记事本程序进行编辑。

(2) 设置系统的预安装显示参数。为了便于叙述,假设磁盘阵列卡驱动程序的文件名为“XXXX.SYS”,在“txtsetup.sif”文件中的“[SCSI]”段增加:XXXX="YYYY"。这项的作用是告诉 WinPE 系统,有一个名为 XXXX 的硬盘控制器是被操作系统所支持的,“YYYY”是对控制器进行注释的内容。

(3) 设置硬件标识。在“txtsetup.sif”文件中的“[HardwareIdsDatabase]”段增加:硬件标识="XXXX"。硬件标识是用来描述被硬盘控制器的硬件标识,是硬件出厂时被写入的,不会改变。硬件标识可以通过以下两个方法获取:一是在驱动程序文件夹中的扩展名为“INF”的文件中查找;二是进入操作系统的设备管理器,查看存储控制器的驱动器详细信息,可以查到硬件标识的信息。

(4) 设置系统挂载驱动参数。在“txtsetup.sif”文件中的“[SCSI.Load]”段增加:XXXX=XXXX.SYS, 4。这行代码表示 WinPE 系统将使用程序“XXXX.SYS”

对服务器阵列卡进行驱动,最后的数字 4 定义了驱动程序存放的目录,可以在“winntDirectories”段中查看。

(5) 设置驱动程序拷贝的具体细节。在“txtsetup.sif”文件中的“[SourceDisksFiles]”段增加:XXXX.SYS=1,, , , , 4_, 4, 1,, 1, 4, 设定了驱动程序拷贝的具体细节。第一个数字“1”代表的是驱动程序拷贝的目标文件夹。

4. 完成 WinPE 系统镜像的制作

完成前面的几项工作后,就可以把 TXTSETUP.SIF 用 ULTRAISO 添加到 ISO 文件里面用以取代之前的文件。或者用 WinCAB 压缩成 CAB 格式,改成 SI_ 扩展名,然后用 ULTRAISO 添加到 ISO 文件里面取代以前的那个 SI_ 文件。再用 WinCAB 软件将修改后的 WINPEO3.ISO 文件进行压缩,然后将其改名为 WINPEWH.IS_,并通过 ULTRAISO 覆盖原先光盘 ISO 镜像中的对应文件。

写到这里,对于普通映像的 WinPE 系统加载 SCSI 驱动程序就可以实现,如果是 WIM 映像格式的 WinPE 系统的话,可以按照以下步骤进行驱动的加载。

使用 DISM 命令向 WIM 映像中添加驱动程序

随着 Windows 操作系统的发展,微软开始使用 WIM 映像格式来进行操作系统的安装,与之相适应的 WinPE 系统也对此做了针对性的改动。早期,主要使用 ImageX 工具来处理 WIM 映像文件,我们需要安装 Windows AIK 来获取 ImageX,也可以从网络上下载到 ImageX。到了 Windows 8 时代,最新版的 DISM 工具经过改进已经具备了 ImageX 原有的功能,并且已经包含在了 Windows 8/8.1 以及 Windows 8/8.1 PE 中。为了把驱动添加进 WinPE 系统,我们可以使用驱动程序服务命令 DISM 来完成这一任务。它可以在脱机映像中用于添加和删除基于 INF 文件的驱动程序,而且可以在处于运行状态的应用程序(联机)上枚举驱动程序,其操作流程如下。

通过使用 DISM 工具将基本映像装载到本地的 Windows PE 目录,假设默认路径在 D 盘。其命令如下:

```
D:>Dism /Mount-WIM /WimFile:winpe.wim /index:1 /
MountDir:d:\winpe-mount
```

通过 Add-driver 将驱动添加进 WinPE 包。在这里要注意两点,一是对于包含很多目录的 Drivers,可以附加

/recurse 来做递归添加；二是对于 Windows 或者早期的驱动，都是没有签名机制的，ForceUnsigned 是必不可少的参数。驱动程序所在路径为：

D:\images\MyDrivers

```
dism /image:d:\winpe-mount /add-driver driver:D:\images\MyDrivers /recurse /forceunsigned
```

添加完驱动程序后，需要将变更提交，并卸载此映像。命令如下：

```
D:\>dism /unmount-wim /Mountdir:d:\winpe-mount /commit
```

这里要注意的是，使用 DISM 工具有两个限制：

一是驱动程序服务命令仅支持 *.inf 文件，Windows Installer 或其他驱动程序包类型（如 *.exe 文件）不受支持；二是如果要添加多个驱动程序，它们将按照在命令行中列出的顺序进行安装。

经验总结

通过反向的方法将服务器的阵列卡驱动程序集成在 WinPE 系统中，同样我们也可以将服务器网卡、主板等驱动程序添加到 WinPE 系统，虽然步骤稍稍有点麻烦，但对于后期的维护还是值得的。

监控远程用户行为

威海 赵永华

了解远程在线用户

在 Windows Server 2012 R2 中如何了解远程用户的在线名单呢？方式有多种，首先可以通过任务管理器 Task Manager，从页面上 Users 栏目可以看到当前登录的用户名单，通过右键菜单 Session 选项，即可甄别哪些是远程桌面用户。另外，通过行命令 quser 也可以解决，需要了解特定的远程服务器时尤其便利，命令为：quser /server contososrv1，其中，contososrv1 指远程服务器。

还有一个命令 qwinsta，不仅可以显示所有登录用户，而且还显示用户登录是通过控制台方式还是通过远程会话方式 RDP session。

限制远程桌面用户使用同一个会话

对远程用户的管理中笔者遇到了这样的情况：当一个用户反复登录远程系统时，系统就会为其分配不同会话，对远程管理造成麻烦，为此需要将其设置为只允许使用同一个会话。具体设置方式如下。

1. 首先需要打开“远程桌面会话主机配置”菜单，为此单击“开始”，依次指向“管理工具”和“远程桌面服务”，然后单击“远程桌面会话主机配置”。

2. 设置“限制每个用户只能进行一个会话”选项：在“编辑设置”区域“常规”下双击“限制每个用户只能进行一个会话”，在“属性”对话框“常规”选项卡选中“限制每个用户只能进行一个会话”复选框，然后单击“确定”。

另外，也可以通过组策略配置限制远程桌面用户使用同一个会话，该组策略设置位于“计算机配置\策略\管理模板\Windows 组件\远程桌面服务\远程桌面会话主机\连接”中，可以使用本地组策略编辑器或组策略管理控制台（GPMC）进行配置。

值得说明的是，此组策略设置将优先于远程桌面会话主机配置中的配置设置。

在 Windows Server 2012 中实现允许多个用户远程桌面登录

Windows Server 2012 默认时允许可运行 2 个用户远程桌面登录，这显然难以满足实际需要，为此，可以通过安装远程桌面会话主机配置来实现 2 个以上用户的远程桌面登录。

1. 首先安装桌面会话主机和远程桌面授权：通过“控

制面板”打开“服务器管理器”，选择“基于角色或基于功能的安装”，在安装界面点击“下一步”。

2. 依次选择“远程桌面服务”以及“桌面会话主机和远程桌面授权”，点击“安装”后重新启动后设置便会生效。

3. 点击“运行→gpedit.msc→计算机配置→管理模板→Windows 组件→远程桌面服务→远程桌面会话主机→授权”，找到“使用指定的远程桌面许可服务器”，设置为启用，并在“要使用的许可证服务器”中设置当前服务器的 IP 或主机名。

4. 点击“运行→gpedit.msc→计算机配置→管理模板→Windows 组件→终端服务”，找到“限制连接数量”，可以设置具体数量。当然，也可设置为 Disable，即禁用（如图 1 所示）。

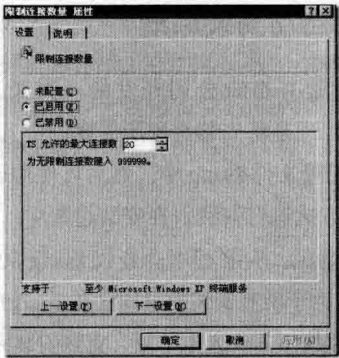


图 1 限制连接数量属性界面

5. 点击“运行→gpedit.msc→计算机配置→管理模板→Windows 组件→远程桌面服务→远程桌面会话主机→授权”，找到“设置远程桌面授权模式”，设置为启用，并在“指定 RD 会话主机服务器授权模式”中选择“按用户”。

6. 单击“运行→gpedit.msc→计算机配置→管理模板→Windows 组件→远程桌面服务→远程桌面会话主机→连接”，可以在“限制连接的数量”中设置最大连接数量（默认无限制）。设置一个用户是否可以使用多个远程桌面连接，选择“将远程桌面服务限制到单独的远程桌面会话”，这里必须设置禁用，否则一个用户只能连接一个远程桌面。

❖ 用 Kickstart 自动安装系统

新疆 马小川

自动安装需求

笔者单位机房需要安装大量的服务器，这些服务器要求安装 Linux 操作系统。如果采用人工安装的方式来安装操作系统，除了需要准备光驱、光盘或 U 盘等安装介质外，还要花费大量的时间进行安装，而其中基本都是重复的工作内容。在机房网络环境中，针对大批量同一安装要求的服务器，相比人工安装方式而言，采用无人值守的网络自动化安装方式无疑是更为便利和有效的。

基于 Kickstart 的网络自动化安装技术，技术架构主要使用了 PXE 网络技术和 Kickstart 的技术。原理是

客户端通过 PXE 网络技术从安装服务器中自动获取 IP 地址、下载映像、加载操作系统，再根据事先设计的 Kickstart 配置文件参数完成系统安装，实现 Linux 操作系统的无人值守安装。同时，由于该技术采用 Client/Server 网络架构模式，所以可以实现同时大批量安装。

基于 Kickstart 的网络自动化安装技术，是比较成熟的技术，在网上有较多的配置实例，有详细的配置步骤，但对原理的介绍却并不详细。本文并不列举实际配置，而是主要针对该安装技术架构的运行原理和步骤进行详细分析和介绍。

Kickstart 自动安装原理

Kickstart 是 RedHat 公司开发的一种无人值守安装方式，工作原理是将安装过程所需要的信息事先记录在 Kickstart 的配置文件 `ks.cfg` 中，然后可使用硬盘、光盘、网络等多种方式进行安装。在安装过程中，当遇到要求填写参数的情况，安装程序会查找 `ks.cfg` 文件，从中查询安装参数。由于所有安装信息均已在 `ks.cfg` 中事先设置，所以安装时系统不需要人工干预，直到安装完成为止。

Kickstart 网络安装，可选择使用 NFS、FTP 或 HTTP 三种方式之一进行安装。NFS、FTP 和 HTTP 服务器中存放系统安装文件（本文用 HTTP 服务器为例进行分析）。

PXE 协议

PXE（Preboot Execute Environment 预启动执行环境）是由 Intel 公司设计的一个网络协议，工作于 Client/Server 的网络模式，它可以使计算机通过网络启动，引导系统网络化安装。协议分为 Client 和 Server 两端，PXE Client 在网卡的 ROM 当中，当待安装系统的计算机开机引导时，BIOS 把 PXE Client 调入内存中执行，PXE Client 会在自检后，以广播的形式发送一个请求，DHCP 服务器在收到请求后会进行回应，给客户端分配 IP 地址，并指示 TFTP 服务器的 IP 地址。客户端在获取 IP 地址后，从 TFTP 服务器中下载开机引导文件“`pxelinux.0`”到本地内存运行，开机引导程序通过 TFTP 读取配置文件 `Pxlinux.cfg`，获取系统初始化的相关文件信息，在内存中进行系统内核和文件系统的加载，随后可开始 Linux 系统安装。配合 Kickstart 技术，可完成 Linux 系统的完全无人值守安装。

Kickstart 网络自动化安装技术架构

使用 Kickstart 网络自动化安装技术，PXE 客户机（即需要安装 Linux 系统的客户机）应该与 DHCP 服务器、TFTP 服务器和 HTTP 服务器都处在同一局域网网段中。在实际应用中，这三台服务器可以都安装在同一台主机上，该主机作为“安装服务器”使用，其中的各项服务并不相互影响，如图 1 所示。

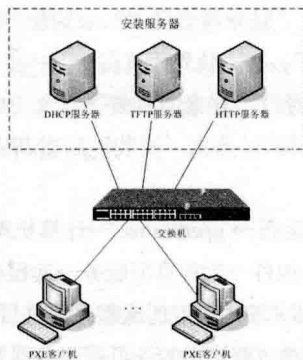


图 1 Kickstart 网络自动化安装技术拓扑图

在 Kickstart 网络自动化安装技术架构中，DHCP 服务器用于 IP 地址分配、指示 PXE 客户机 `pxelinux` 启动程序和配置文件的下载地址。TFTP 服务器用于放置 `pxelinux` 启动程序和配置文件，PXE 客户机从 TFTP 服务器上下载并执行 `pxelinux` 引导程序，在内存中加载系统内核，构建一个基本的操作系统。HTTP 服务器用于放置系统安装镜像和 Kickstart 的配置文件。在客户机内存中已构建的基本操作系统，从 HTTP 服务器中读取 Kickstart 配置文件“`ks.cfg`”，根据该配置文件执行安装程序，从 HTTP 服务器中读取系统安装镜像，在硬盘上安装操作系统。在系统安装过程需要进行设置参数时，程序自动根据“`ks.cfg`”文件中的配置完成参数设置，最终完成 Linux 系统的安装。Kickstart 网络自动化安装步骤如图 2 所示。

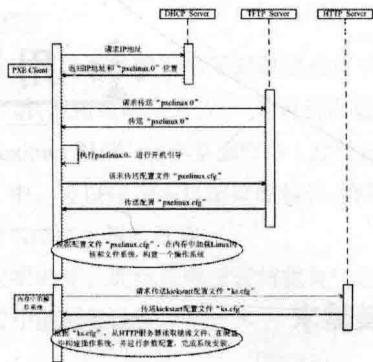


图 2 Kickstart 网络自动化安装步骤图

使用网络自动化安装 Linux 系统的客户机，必须开放网卡的 PXE 启动功能。目前几乎所有网卡都具备 PXE 启动功能，但客户机 BIOS 中有可能将此功能默认设置为禁止启动的。在进行安装之前，需要将该功能开放。

经验总结

基于 Kickstart 网络自动化安装技术，主要用到了 PXE 网络技术和 Kickstart 技术。PXE 网络技术主要负责客户机安装程序的引导和内核加载，为系统安装做好初始化准备。Kickstart 技术则负责 Linux 操作系统的安

装和配置。本文主要对 Kickstart 网络自动化安装技术的原理进行了分析和介绍。在实际运维工作中运用这种技术，可以有效地减少大规模安装 Linux 操作系统的工作量，提高维护效率。

构建收入合同管理系统

长春 王旭

笔者单位随着企业的转型升级，企业项目中包涵的合同及合同相关其他业务的管理工作也逐渐增多，传统的合同管理模式已经开始显现出对新环境、新需求的不适应。计算机网络的发展和普及不断推动着各类管理信息系统的开发和应用，运用企业先进的网络硬件环境及卓越的技术水平，充分利用信息化管理手段，开发管理系统对合同及相关业务进行管理，可以大幅提升管理质量和效率。

收入合同管理系统运用计算机技术和数据库技术，将人力资源、财务信息和生产项目结合起来，实现合同的信息化管理，系统采用 B/S 架构进行开发，整个系统实现了两个主要内容：在研究设计方面，应用符合我单位传统开发模式的软件开发技术对收入合同管理系统完成模型的建立和功能模块的实现；在应用与实践方面，以实际需求作为开发基础，并将合同管理方面的历史数据与管理问题进行整合与改造，开发出实用、简洁的管理系统。

建设背景

随着现代科学技术的飞速发展与广泛普及，市场上已经存在了非常成熟的合同管理系统软件，但是由于不同的企业对自己的合同管理业务流程有着不同的理解和管理方式，所以没有任何一个成形的系统可以作为通用的系统进行使用。因此，根据笔者单位具体情况，决定首先开发收入合同管理系统，范围涵盖所有有费用收入的合同，及这些收入合同相关的业务工作，例如合同的

会签、变更、收费、执行、发票开具等工作。

研究与实践

根据工作需要及目前的工作重点和业务划分，将合同的管理主要分为收入合同和支出合同，本次率先开发全院的收入合同管理系统，系统的模块功能如图 1 所示。

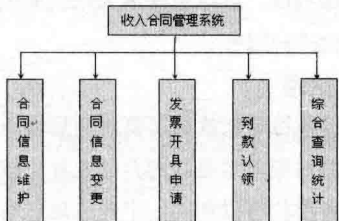


图 1 系统模块功能

1. 收入合同信息维护、信息变更

合同管理系统最基础的功能就是合同的基本信息录入，合同的基本信息包括合同分类号、合同编号、甲方、合同金额、合同电文本及附件等三十余项基础信息。基础信息字段越完整、丰富，后期的各种统计、查询功能越方便、强大。

工程项目在开始时需要下达工程项目任务卡，从而开始实施下一步工作。此次开发收入合同管理系统所要解决的主要问题就是将工程项目任务卡与合同进行关联，这两项信息的关联对今后规范管理合同与项目、合同的执行情况、财务成本状况都有着积极的影响，是多项管理工作质量提升的基础性工作。

合同的基本信息由经营人员录入完成后,需要在系统中完成合同的传审流程,经市场部、项目经理、分公司总经理、三标部、计法部、院领导审批完成后形成正式的合同记录,供合同管理系统的其他模块进行使用。

在合同录入及完成传审流程后,对需要进行合同变更的记录进行变更操作,合同的变更包括“合同金额”、“合同甲方”、“合同范围”、“合同条款”等多项变更方式。同样,合同变更也需要市场部主任、计法部、三标部及公司分管领导审批完成后才可以正式生效。同时同步到合同的基本信息中,在其他的查询统计功能中显示的是变更后的各种信息。

2. 发票申请

系统优化了发票申请内容和申请流程,将发票申请时所添写的开票合同、合同的甲方与合同基本信息进行强关联,不由开票人手工进行添写,避免了后期对开发票进行统计时,合同名称或合同编号书写错误导致无法统计总开票金额的问题。

发票开具流程的最后环节是由财务的工作人员进行开具发票,在此环节增加了精拍仪拍摄发票的功能,精拍仪与合同管理系统进行了无缝的连接,拍摄完成后直接上传到发票开具流程,避免因单方面弄丢发票而产生不必要的纠纷。这种管理方式相比以前的手工管理提高了管理的精细程度,可以更好地为全院的生产人员及外方的业主单位进行服务。

3. 到款认领

工程项目的每笔来款都需要对应到惟一的合同,但来款和合同的对应关系是以前合同工作中较为模糊的部分,由于笔者单位可以和同一个业主单位有多个工程上的业务往来关系,业主单位的来款记录并不明确地指出具体合同;来款记录的付款方和登记的业主名称不统一等原因,导致在整理来款对应合同时非常困难,往往会有大量的来款滞留在财务部门,这使单位的诸多合同无法完结,对合同的收入统计产生巨大的影响。

在收入合同管理系统中开发了到款认领的流程,当登记来款记录时,由系统自动将认领任务发送到开具过这个来款业主的发票记录的人,由这个人认领这笔来款。这种方式可以及时并且较为准确地认领来款,从而解决

来款和合同难以对应的问题。

4. 综合查询统计

收入合同管理系统改变了以前各个系统只提供简单几个查询字段的查询方式,重新设计了以目前主流查询方式为基础方式的查询系统,提供了丰富的查询条件字段,字段组合方式及广泛的取值范围。可供使用部门按时间段、按部门、按合同类型等多种条件查询所有的合同所具备的基本信息,包括到款、发票等。

经验与体会

从系统最终的开发成果来看,此次开发的收入合同管理系统完成了全院合同基本信息的录入、修改、删除、会签、归档、查询功能。另外,还包括合同的发票开具、到款认领等功能。这两部分从合同管理角色来讲是目前使用最为急迫的。

整个系统开发完成并不是整个项目的结果,笔者单位在六十年的生产工作中积累巨大数量的合同数据,发票数据及其他与合同业务相关的周边数据,建立收入合同管理系统就是要管理这些数据,所以,将这些大量的历史数据整合到新开发的系统中并加以结构化的利用,才是本次项目的根本目的。

历史数据的导入处理是这次项目的另一项艰巨任务,由于合同数量巨大而且很多数据是非结构化的,一部分整理工作只能由人手工进行完成,再由软件开发人员进行整合导入,这次历史数据的导入工作持续一个月之久,其中运用到了很多方式、方法,对以后涉及到的历史数量处理工作提供了极大的帮助经验。

合同管理系统与企业的组织机构变更、运营模式的变化、生产体系的发展都具有密切的联系,收入合同管理系统是对今后开发管理全院所有类型合同的一次尝试,通过将合同进行信息化的管理,将涉及合同及生产业务的周边工作进行信息化的优化,将原来分散的工作单元统一在一起,真正做到用信息化的方法管理和辅助生产,实现为决策层进行统计分析、形成上层决策提供重要依据,这也是信息化建设的最终目标。



NTP 服务统一终端配置

安徽 冯驰

笔者单位 ERP 上线成功,信息安全面临了新的问题。所有系统全部一级或二级部署,用户登录全部通过一个账号完成。为保证安全,系统要求在用信息系统、设备时间必须全网统一,为了方便管理,使系统的安全管理、日志分析、应用系统等工作的参照时间做到一致,需要建设统一的 NTP 时间服务环境。

可选的 NTP 方案

NTP 功能的实现手段有多种,各种方法及优缺点比较如下。

1. 使用具备卫星时钟、原子时钟等高精度时间源的专用服务器,精确性好,成本较高。
2. 采用 Windows 自带的 NTP 服务实现,操作较为简单,但服务的可控性较差,手段较少。
3. 采用 Windows 平台上的第三方服务软件实现。
4. 采用 Linux、Unix 平台上的 NTPD 服务来实现,NTPD 服务较为成熟,可配置的参数较多,对服务的控制粒度较细。
5. 采用核心网络设备提供 NTP 服务,服务的可控性、兼容性较差。

服务端建设方法设计

依据地市公司的特点,我们决定采用 Linux 平台上的 NTPD 服务来实现系统的建设。

1. 系统安装

本次采用了 Redhat/CentOS Linux 系统,主要安装过程依次为介质引导系统,按回车开始安装。连续两次点击 Next,根据需求设置分区。设置 IP 地址,选择好安装包组件,系统将开始安装过程。

2. NTPD 服务端设置

确认 NTPD 服务已经开启,时区设置正确。确认

NTPD 能够作为客户端从上级 NTP 服务器获取时间。

NTPD 服务的主要配置文件默认是 /etc/ntp.conf。设置配置文件中的“restrict”项,主要用于控制客户端对服务器的访问,一般设置如下所示:

```
restrict default kod nomodify notrap nopeer noquery
# 禁用全部地址对 NTPD 各服务的访问
restrict 127.0.0.1
# 允许本机地址 (127.0.0.1) 对 NTPD 各服务的访问
restrict xx.xx.xx.xx mask xx.xx.xx.xx nomodify
# 允许设置的可信任地址段对 NTPD 各服务的访问,但不允许此地址段内客户端修改 NTPD 服务器时间 (nomodify)。
```

设置配置文件中的“server”项,主要用于 NTPD 的上级服务器、本机时钟的同步,以及时钟的层次 stratum:

```
server 127.127.1.0
#NTPD 把本地主机的时钟也看作外部时钟源来处理,分配的地址是 127.127.1.0
fudge 127.127.1.0 stratum 1
# 设置本地时钟源的层次为 1,这样如果 NTPD 服务从本地时钟源获取时间的话,NTPD 对外宣布的时间层次为 2。
```

Server NTP 的 IP 地址

配置完毕,重启 NTPD 服务,使配置更改生效。

设置客户端

1. 普通 Windows 系统下的 NTP 客户端设置

打开“控制面板→日期和时间”,选择“Internet 时间”选项卡。选中“自动与 Internet 时间服务器同步”选项,在“服务器”栏目中输入 NTP 时钟源的 IP 地址或域名,点击“立即更新”按钮进行一次时间同步,系统提示“与

XXX 同步时间成功”表示设置正确。

点击“确定”按钮，完成设置。

2.Windows 系统域环境下的 NTP 客户端设置

(1) 配置域控制器的时间同步，运行“net time /setsntp:ip 地址”，使 sntp 服务指向 NTP 服务器，运行“net time /querysnpt”，确认设置生效。

(2) 在域成员服务器上，运行“net time /domain /set”，设置服务器从域控制器同步时间。

(3) 重新启动服务器上的“windows time”服务。

(4) 在服务器上执行“w32tm /resync”，立即进行一次更新。

3.Redhat/CentOS 下的 NTP 客户端设置

(1) 选择正确的时区

在控制台运行“cat /etc/sysconfig/clock”命令，检查时区是否为“Asia/Shanghai”，如果不是，运行 system-config-date 命令，重新设置时区为“Asia/Shanghai”。

(2) 与时间服务器进行一次同步更新

在控制台运行“ntpdate -u NTP 的 IP 地址”命令，再执行“date”命令，检查系统时间是否成功更新。

(3) 确认 ntpd 服务

运行“ntsysv”命令，检查 ntpd 服务是否被选中，如果服务未被选择，则选中 ntpd 服务，并执行以下操作：

执行“vi /etc/ntp.conf”，编辑以 restrict 开头的控制 IP 地址段的行，内容改为“restrict 127.0.0.1”。删除所有以 server 开头的行，在原有位置增加一行“server NTP 的 IP 地址 prefer”，保存退出。

执行“vi /etc/ntp/step-tickers”，添加一行“NTP 的 IP 地址”，保存退出。

执行“vi /etc/sysconfig/ntpd”，修改“SYNC_HWCLOCK=yes”，保存退出。

执行“/etc/inet.d/ntpd start”，启动 NTP 服务。

4. 检查 NTPD 服务状态

使用 ntpstat、ntpq -p 命令检查 NTP 协议同步状态。

export NTPDATE_SERVER= NTP 的 IP 地址

export XNTPD=1

export XNTPD_ARGS=

2. 生成 /etc/ntp.drift 文件，执行命令 touch /etc/ntp.drift。

3. 修改 /etc/ntp.conf 文件，包括如下内容：

server NTP 的 IP 地址

driftfile /etc/ntp.drift

4. 启动 NTP 服务，执行命令 /sbin/init.d/xntpd start。

5. 检查 NTPD 服务状态

使用 ntpq -p 命令检查 NTP 协议同步状态。

Cisco 网络、安全设备 NTP 客户端设置

1. 设置时区，执行 clock timezone Beijing 8。

2. 设置 NTP 协议

config terminal

ntp source xxx (设置用来和 NTP 服务器通信的接口)

ntp server NTP 的 IP 地址

华为网络设备 NTP 客户端设置

1. 设置时区，执行 clock Timezone Beijing add 08:00:00

2. 设置 NTP 协议

ntp-service source-interface Vlan-interface xxx

ntp-service unicast-server NTP 的 IP 地址

clock Timezone Beijing add 08:00:00

经验总结

通过实现 NTP 服务，采集上级的一级 NTP 服务，并为全公司的信息安全设备实现时间同步。公司网络设备、服务器设备、PC 客户端从相应级别 NTP 服务器获取时间，实现信息系统的时间准确、统一，为 SG186、ERP、信息安全的安全稳定运行提供了保障。

HPUX 系统下 NTP 客户端设置

1. 编辑 /etc/rc.config.d/netdaemons 文件，文件内容设定如下：

在存储虚拟机迁移数据

▼ 武汉 米泉 严迪 陈浩 闵克锋

数据迁移是各企业单位 IT 建设经常面对的工作。当今数据迁移的主要难题是进行一次成功的数据迁移时间要求越来越短。然而应用在存储方面的需求不断增加,存储的升级和更替更加频繁;同时,企业的应用趋向于全年不停顿运行、对系统的可靠性、可用性要求不断提高,维护时间窗口的不断减少等因素,使得进行一次平滑的成功数据迁移越来越具挑战。某汽车制造公司在新数据中心迁移的过程中,利用多种数据迁移技术,完成了各应用系统的迁移工作。其中,基于存储虚拟机的数据迁移技术,为首次使用。

常见数据迁移技术

对于数据的迁移,目前主要采用如下五种方法:

基于主机操作系统逻辑卷镜像技术的数据迁移

基于数据库备份和恢复技术的数据迁移

基于应用层工具的数据迁移

基于磁盘阵列远程数据复制技术的数据迁移

基于存储虚拟化技术的数据迁移

基于主机逻辑卷镜像技术的数据迁移

此种数据迁移方法,主要利用业务主机操作系统内置的逻辑卷管理系统的逻辑卷镜像(LV Mirror)技术,可以保证业务数据在原有的磁盘阵列和新的磁盘阵列上保持同步,两边数据完全一致。此种方法存在如下优点:

步骤简单,容易实现,速度快;

不需要考虑到上层数据应用系统的内部的结构;

可以在线进行,只需要较短的停机时间;

但是,利用这种方法,也存在如下的问题:

在进行初始化数据同步的时候,会对在线系统的性能造成较大的冲击;

只适合部署了逻辑卷管理系统的主机,主要是小型机。

基于数据库备份和恢复技术的数据迁移

此种数据迁移方法,主要通过数据库自带的备份和恢复功能以及逻辑日志追加的技术,实现一个数据逐步迁移的方法,最后达到把数据从原有的磁盘阵列完全迁移到新的磁盘阵列的目的。本方法比较安全,当数据迁移不成功时,不影响生产系统的正常运行,但是迁移时间较长,对技术要求较高,而且需要专门用于数据迁移的一台与生产主机环境一样的主机,硬件配置可以稍低一点。

基于应用层工具的数据迁移

此种数据迁移的方法,利用一些第三方的工具实现数据迁移,如文件系统层面实现的 Veritas 的 VVR,虚拟化平台层面实现的 VMware vMotion 等。这些方法都是特定应用的针对性工具,对特定应用比较好用,但需要满足一些前提条件,如 Veritas 的 VVR 只能基于 VxFS 文件系统上的卷复制,对于其它的文件系统或 raw device,则无法使用。

基于磁盘阵列数据复制技术的数据迁移

此种数据迁移方法,可以在同一个磁盘阵列内通过基于磁盘阵列的克隆软件或卷迁移软件实现数据复制,完成数据迁移。可以实现在两套磁盘阵列之间的数据迁移,并且此种方法不占用主机资源,对应用透明。但是源磁盘阵列和目标磁盘阵列必须是同一厂家的同一系列的产品,而且迁移过程对生产系统有一定的性能影响。

基于存储虚拟化技术的数据迁移

基于存储虚拟化技术的数据迁移,主要是解决异构存储间海量数据迁移难题。该技术继承了存储层进行数据迁移的应用透明、迁移效率高的优势,与此同时在虚拟化基础上将原来不能完成数据复制的存储设备整合在一起,形成统一存储池,这时物理上在两个磁盘的数据卷之间的迁移,在逻辑上来讲是在整合虚拟后的同一个磁盘阵列内卷迁移。由于不涉及主机的任何设置修改,实施比较简单,迁移速度非常快。此数据迁移技术方案示意图如图 1 所示。

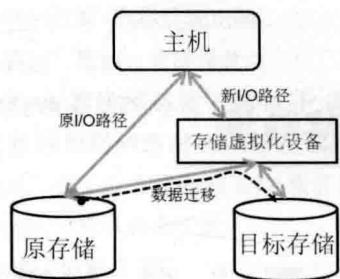


图1 常见的基于存储虚拟化的数据迁移方案

但是，这类数据迁移方法的前提是需要对原有存储实施虚拟化，涉及存储路径的改变，主机对存储 LUN 的重新识别，因此存在业务停机窗口，无法实现不停机数据迁移。

总体上，基于主机逻辑卷镜像技术的数据迁移、基于数据库备份和恢复技术的数据迁移、基于应用层工具的数据迁移都属于基于主机服务器层的迁移技术；基于磁盘阵列数据复制技术的数据迁移、基于存储虚拟化技术的数据迁移都属于基于存储层的数据迁移技术。

基于存储的数据迁移是一次性的将数据从一个存储转移到另一个存储系统上，它包括对新存储的启用和数据可用性的保证。在一些情况下，基于存储的数据迁移是进行数据大集中的手段，非常适合大规模数据迁移需求，因此被许多数据迁移项目采用为主要迁移手段。

基于存储虚拟机的不停机数据迁移技术及迁移方案步骤

鉴于一般的存储虚拟化迁移技术无法实现不停机数据迁移，迁移过程无法近自动化，业界开发出更具创新性的存储虚拟化技术，来优化数据迁移过程以保证业务连续性。下面对这种创新技术方案做具体介绍。

这种数据迁移技术基于创新的存储虚拟化技术——Virtual Storage Machine (VSM) 虚拟存储机技术。这种技术创造性地将服务器虚机的概念引入存储，在一台物理存储内允许用户按照业务和应用的要求定义多个 Virtual Storage Machine (VSM)，VSM 与一台存储类似，具备自己的存储 ID，设备序列号和端口 WWN，通过 VSM 的定义，能虚拟化一台物理的存储阵列，因此，服务器不会察觉到所使用的资源实际上是分布在不同的存储设备中。

借助虚拟存储的技术，数据源存储设备的 ID 被完整地复制到数据目标存储设备上，而服务器无法察觉存储设备物理身份的变化，这一过程对任何操作系统、虚

拟机监控程序，服务器、服务器的路径管理软件，服务器集群软件以及存储网络连接等都是透明的。具体原理如图 2 所示。

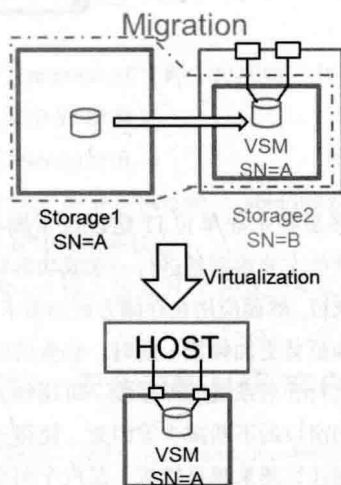


图2 基于 VSM 存储虚机的数据迁移技术原理

接下来，具体阐述利用 VSM 虚拟存储技术进行数据迁移的具体步骤。

如图 3 所示，原存储 (ID:#175 00) 上的数据，比如 SCSI 标识为 10:00 的 LUN 上的数据迁移到目标存储 (ID:#20700) 的 SCSI 标识为 22:00 的 LUN 上。目标存储具备 VSM 虚拟存储功能。

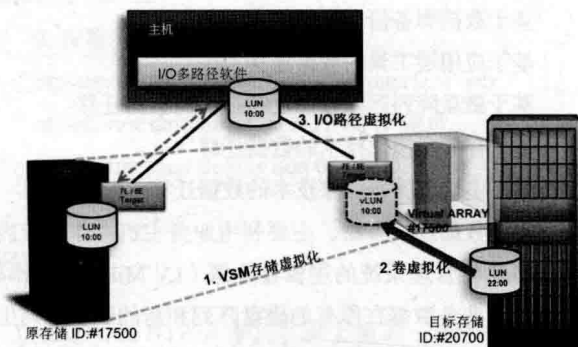


图3 基于 VSM 存储虚机进行数据迁移步骤示意图一

第一，利用目标存储的 VSM 功能，在目标存储上创建一个与原存储具备相同标识 17500，包括设备及 FC 网络标识的 VSM 设备；

第二，利用传统的卷虚拟化功能，将目标存储上的 LUN 22 : 00 在 VSM 17500 上创建一个虚拟卷，LUN ID 与原卷 10:00 一致，但物理空间是目标存储的 LUN 22 : 00 ；

第三，将目标存储和目标卷与主机建立路径，作为

同一逻辑路径下的物理备路径，主机感知路径无改变，I/O 无影响；

第四，建立原卷 LUN10:00 与目标卷的 LUN22:00 的数据同步关系，运用的技术是传统的卷复制与拷贝技术；

第五，待数据同步完毕，原卷 LUN10:00 与目标卷的 LUN22:00 的数据完全一致，断开主机与原存储的连接，I/O 的逻辑路径依然没变，实质上是把主路径由原路径切换为之前的备路径；主机与目标存储之间的路径，因此，这种切换对业务无影响，数据迁移完毕。

四、五步骤可如图 4 所示。

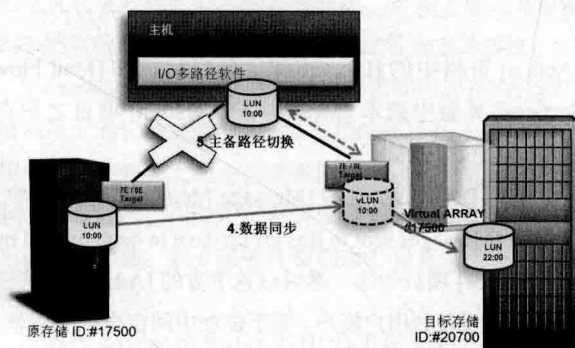


图 4 基于 VSM 存储虚机进行数据迁移步骤示意图二

以下是对各数据迁移技术的对比评估。

卷镜像迁移方案

较短的停机时间；可以根据业务情况，LUN 级别，可灵活控制拷贝速度；需要消耗较少的主机端资源（文件系统层次镜像），业务高峰时性能下降 >10%；完全采用系统管理员熟悉的文件系统命令，难度很小且易控制。

Oracle Standby by 方式备份和恢复

停机 2 次；速度和性能中等；需要消耗一定的主机端资源（数据库层次 log）；实施难度取决于对数据库的熟悉程度（注意数据库的 no log 操作）。

磁盘阵列复制

停机 1-2 次；速度较快，但不能灵活调节；需消耗阵列的控制器能力和大量缓存资源；主机 IO 需增加一定的时延，若在同机房迁移则影响较小；需仔细规划，确保阵列和主机之间的数据完整性；迁移结束后测试验证可回退性差。存在安全隐患，实施案例很少。

VMware Storage Vmotion 迁移方案

停机 2 次；速度可控；需要占用 5-10% 的主机系统资源；实施难度取决于数据迁移服务人员实施能力。

存储虚拟化 + 卷同步

停机 1 次，迁移完成后的 I/O 切换速度很快，非常灵活；不消耗任何主机资源，需消耗阵列的控制器能力

和大量缓存资源；主机 IO 需增加微不足道的时延，总体在 2ms 内；需要将外部存储 FC 端口和目标存储逻辑连接，以便能识别和虚拟化外部存储的 LUN。然后通过卷迁移将外部存储的卷在线迁移到目标存储内部。每一步需要手工操作，无法脚本自动化。

基于 VSM 的数据迁移

无计划停机时间，可全部在线实施；速度很快，非常灵活；不消耗任何主机资源，需消耗阵列的控制器能力和大量缓存资源；主机 IO 需增加微不足道的时延，总体在 2ms 内；需要将外部存储 FC 端口和目标存储逻辑连接，以便能识别和虚拟化外部存储的 LUN。之后具体迁移操作可近自动化操作。原存储上的其它配置也自动迁移到新存储上，大幅减少了实施工作量。

数据迁移项目实践及效益评估

数据迁移项目实践

某汽车制造公司现有各种数据类型及特点的应用系统。如公司最核心的业务 SAP 系统，全年无休的商务 CRM 系统，非结构化数据的 workspace 系统，大数据量的数据仓库系统，基于 VMWare 虚拟化构架的应用系统。

方案选择

在各类应用系统中，SAP 系统是公司最核心的应用系统，包含了企业运营最重要的数据，同时也是数据量较大的一个系统。SAP 系统约有 6TB 的数据，在原有的存储上分配了 15 个 LUN。类似 CRM 系统这种公司商务领域最重要的系统，总计约有 5TB 的数据，但应用的特性决定了该应用是不允许有停机时间的。如数据仓库系统这种数据量最大的分析、决策型系统有约 10TB 的数据。数据量决定了数据迁移的效率要求。

根据这几类系统的特殊性 & 业务要求，选择基于 VSM 技术的数据迁移方案完成了数据迁移，相比较传统的数据迁移方案来说，VSM 的优点在于迁移过程中，应用系统是几乎感知不到的。同时，也减少了约 16-20 小时的迁移时间和近 90% 的迁移工作量，并且降低了因停机导致的业务中断及数据错漏的风险，降低了因迁移对业务使用造成的性能影响，确保了整个数据迁移的安全、高效。

结语

数据迁移在数据中心里是高概率任务，不仅需要投

入相当的资源，而且伴随着很大的实施风险，实际上 IT 部门可以参考最佳实践经验并借助创新技术来减少投

入、降低风险。基于 VSM 的存储虚机的 NDM 就是这样的创新技术，用来帮助 IT 用户实现目标、保持竞争力。

Exchange 2010 邮件管理秘诀

▼ 顾武雄

有鉴于企业对于邮件平台在合规性管理需求上的极度重视，让 Microsoft 打从前一版的 Exchange Server 2007 中，便提供了因应各种不同层面需求的内建方案，这一些包括了邮件存档管理、邮件生命周期管理、以及集成数字版权管理等等解决方案。而在目前全球最多企业使用的 Exchange Server 2010 版本设计中，为了更加强化企业在合规性上的高级管理需求，并且提供 IT 部门更低支持成本的解决方案，因此特别改善以及新增了几项在合规性管理上的新特色，这分别是邮件发送的审阅管理、客户端邮件存档管理、客户端邮件保留策略设置、多重邮箱的探索、集成 AD RMS 的传输规则设置。接下来就让我们一起来学习几个关于邮件安全的高级管理技巧。

电子邮件发送前的审阅管理

许多公司对于重要文的制作到发布（例如：产品文件），都必须经由特定的主管来审核。如今对于一些重要的电子邮件发送，各部门主管也希望能够有这样的审核机制，不知道在最新的 Exchange Server 2010 中是否有提供这一项管理功能。

目前在 Exchange Server 2010 中所新增的邮件发送的审核机制，让一般用户在将邮件寄送给特定重要的客户、合作伙伴或是其他部门的通讯群组时，自动转交给预先指定好的审阅者来进行检视与审核，有效确保重要邮件属性发送的正确性与安全性。接下来就让我们一同了解一下这一项管理功能的使用。

首先请在 Exchange 管理控制台中点选至 [Recipient Configuration][Distribution Group] 项目节点上，接着针对现有所要准备设置审阅的通讯群组项目，点选位在

[Action] 窗格中的 [Properties]。开启后请在 [Mail Flow Settings] 页面中选取 [Message Moderation] 项目之后点选 [Properties] 继续。

来到如图 1 所示的 [Message Moderation] 页面中，请先将 [Messages sent to this group have to be approved by a moderator] 项目勾选，然后点选下方的 [Add] 按钮来选择作为审阅者的用户帐户。至于位在中间窗格中的清单，则是可以设置哪些用户的邮件发送至此通讯群组时不需要经过审阅。

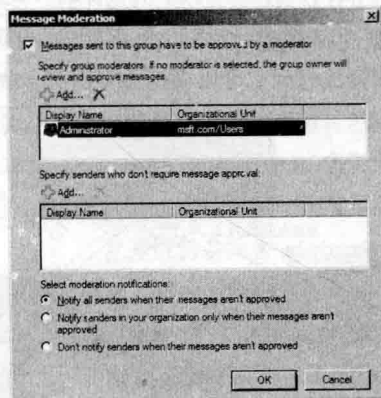


图 1 邮件审阅设置

最后您可以在本页面的下方三个选项中来决定审阅邮件的通知方式，由上而下依序说明如下：

当所发送给此通讯群组的邮件被审阅者拒绝时，自动发送 E-mail 通知所有发送者。

当所发送给此通讯群组的邮件被审阅者拒绝时，仅自动发送 E-mail 通知属于组织内的发送者。

当所发送给此通讯群组的邮件被审阅者拒绝时，不要自动通知任何发送者。

完成通讯群组中的邮件审阅设置之后。当有用户寄送 E-mail 到此通讯群组时，审阅者便会收到类似范例中

的通知邮件,这时候可以点选附件档案链接来检视用户所寄送的 E-mail 属性。等到确认其属性之后,再透过点选 [Approve] 或 [Reject] 来决定要核准还是拒绝。

如何解决 E-mail 存档的问题

目前许多企业客户端几乎都采用本地 PST 档案的方式来管理个人的 E-mail 存档,在运作管理上每当档案不断成长越来越大时,便会降低 Outlook 的运作效能。至于如果将它移动到域络共享的文件夹中,则还会进一步衍生其它更多难以处理的各种状况,增加无法正常存取 PST 档案的问题,以及造成存档属性管理上的难度。

Exchange Server 2012 的用户邮箱邮件的存档管理功能,对于成长至大型的 Email 存档邮箱 (10-100 GB) 的使用则效能表现上是不会受到影响的。并且是集中在伺服器端来管理的,而对于配置设置管理上也是与现有的邮箱区分开来的。接下来就让我们来看看有关于这部分的相关操作说明。

请在 Exchange Server 2010 的管理控制台中,我们可以针对现有的用户邮箱项目,点选位在 [动作] 窗格中的 [Enable Archive] 功能,紧接着点选 [Yes] 按钮来确认建立这个用户专属的存档邮箱。

完成了用户专属的存档邮箱建立之后,接下来我们可以开启这个用户邮箱的属性属性,然后如图 2 所示切换到 [Mailbox Features] 页面,便可以看到 [Archive] 功能的启用状态,若想要变更它在 Outlook 与 OWA 的显示名称,请点选 [Properties] 按钮继续。

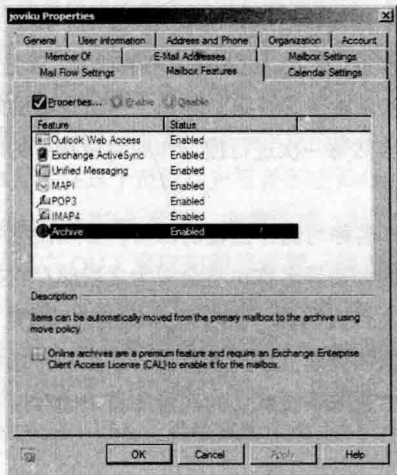


图 2 查看邮箱功能设置

在 [Archive Properties] 页面中,可以变更存档邮箱的显示名称,这个名称将会自动显示在 OWA 与 Outlook

的联机中。切换到 [Mailbox Settings] 页面中,在选取 [Archive Quota] 项目之后点选 [Properties] 按钮,则可以设置有关于存档邮箱本身的配额空间。

完成了以上有关于用户存档邮箱的建立与设置之后,接下来只要以该用户的帐户,透过 OWA 或 Outlook 2010 来进行联机。您将会发现除了原有的邮箱之外,也自动完成了附属存档邮箱的联机了。

电子邮件保留策略功能使用

在前一版的 Exchange Server 2007 中,对于邮件生命周期的管理需求部份,我们都是透过邮件记录管理 (MRM) 功能,来统一管理客户端各项默认邮件文件夹或是自定义文件夹的保留策略 (例如:客户服务邮件文件夹),然而这项机制毕竟是由 IT 部门来统一管理,客户端用户本身是无法自行针对自己所建立的邮件文件夹,或是个别的邮件项目来选择所需要的保留策略。因此想了解在 Exchange Server 2010 中是否有更好的功能来解决这一问题。

全新 Exchange Server 2010 所提供的全新邮件生命周期的管理功能,已经可以让用户自行针对个别的邮件文件夹,或是个别的邮件邮件来设置不同的邮件保留策略。而策略的定义则是由 Exchange 伺服器端来集中设置后再应用至客户端用户,用户只要在客户端的操作接口中即可选择与应用。

接下来让我们来看看如何自定义邮件保留策略。首先我们必须建立各种不同需求的邮件保留标签,必须开启 Exchange 命令控制台,然后以 New-RetentionPolicyTag 命令及相关参数来建立。

当我们完成了各种需要的保留策略标签之后,便可以开始将它门加以归类处理,以便于进行后续应用在特定用户邮箱的设置上。必须下达 New-RetentionPolicy 命令以及 RetentionPolicyTagLinks 参数来加以设置,而每一个保留策略标签之间使用逗号区隔开来即可。

最后便可以透过 Set-Mailbox 命令搭配 RetentionPolicy 参数来设置保留策略,以便将前面所建立好的保留策略应用到指定的用户邮箱。如果想进行批次用户邮箱的应用,则必须透过管线搭配 Get-Mailbox 与 OrganizationalUnit 参数来应用至指定的组织单位,或是使用 Get-User 搭配 Filter 参数来与 Set-Mailbox 命令,将策略应用到例如特定的部门用户邮箱之上也是可以的。

最后建议您去看看被保留策略应用后的客户端联机情形。您只要在用户登入 OWA 之后,针对任一个邮箱文件夹,按下鼠标右键从 [Retention Policy] 子选单中,来选取想要应用的保留策略标签,而不同保留策略卷标项目会有不同的保留时间与相对的运行动作。

另外您也可以透过 Exchange 伺服端的传输规则定义,来设计应用指定的默认策略项目在指定的通讯群组或用户上,或是可以针对特定的 Email 属性条件(例如:属性关键词)来应用。

多重电子邮件邮箱审核管理

企业中中有许多信息方面的管理工作并非全部都是隶属于 IT 人员的工作职责,可是他们通常又无法透过一般 IT 管理工具,去存取与设置电子邮件服务器的权限,来进行相关邮件审核的管理工作。因此如果想在 Exchange Server 2010 中,让非 IT 的人员可以来进行邮件审核的管理工作,该如何做呢?

在全新 Exchange Server 2010 中,在搭配以角色为基础的存取管理功能下,提供了跨邮箱搜寻的用户接口,来赋予法规管理者以及人力资源管理者等特定需求的用户,能够轻易的针对所选取的用户邮箱来进行各种条件的属性搜寻,例如特定的主题、属性关键词或是特定范围日期时间内的邮件等等。针对这一项探索功能我们称它为 e-Discovery。接下来让我们来看看有关于 e-Discovery 这一项功能应用的实作说明。

首先我们必须建立一个准备用来储存探索结果邮件项目的专属邮箱。必须在 Exchange 命令控制台中下达 New-Mailbox 命令来建立,其中务必加入 -Discovery 参数设置,如此一来才能够建立属于探索类型的邮箱。

接下来必须使用系统管理员开启进入到 Exchange 控制台 (ECP),例如您可以输入类似 <https://exch2010.contoso.com/ecp> 地址来进行联机,当然您也可以选择从 Exchange 管理控制台中的 [工具箱] 来开启此网页。在的 [系统管理员角色] 页面中,请在选取 [Discovery Management] 角色项目之后点选 [详细资料] 继续。在 [Discovery Management] 成员设置页面中,可以先看到在这个角色群组中已包括了两个角色权限,分别是 [Legal Hold] 与 [Mailbox Search]。请点选 [新增] 按钮来将所要赋予探索管理员角色群组权限的用户加入即可。

注意

请注意!即便是系统默认的 Administrator,若不是隶属 [Discovery Management] 成员,一样是无法进行多重邮箱探索作业的。

一旦完成了 [Discovery Management] 角色群组成员的设置之后,该用户便可已在登入 Exchange 控制台页面之后从 [报告] 节点项目中看到可以使用 [邮箱搜寻] 这一项功能。在此您可以看到所有建立过的搜寻设置项目,并且可以随时针对任一项目运行再一次的搜寻作业,如果想要修改现有的搜寻项目设置,请针对该项目点选 [详细数据] 即可。接下来让我们点选 [新增] 按钮来建立一个搜寻设置试试看。

接下来将会开启 [新增邮箱搜寻] 的页面,首先必须设置所要搜寻的关键词,可搭配双引号以及大写的 AND、OR 以及 NOT 来作为分隔的字词,如果想要让可能无法进行搜寻的项目也进行搜寻(例如:加密的附加档案、无法辨识的附件档案),请将 [包含的项目无法进行搜寻] 设置勾选即可。

接下来您可以点选 [选取邮件类型] 按钮,来开启 [要搜寻的邮件类型],在此您可以直接选取 [搜寻所有邮件类型,包括可能未列于下方的类型在内] 项目,或是在下方中选取特定的几项要搜寻的项目类型,例如只针对电子邮件以及会议的属性来进行搜寻,在默认的状态下只会针对 [电子邮件] 类型进行搜寻。

在日期范围设置部份,您可以设置所要搜寻的邮件项目日期范围,只要设置开始与结束的日期即可,在默认的状态下是没有启用日期范围设置的。接下来在要搜寻的邮箱部份,您可以选择搜寻所有邮箱,或是点选 [新增] 按钮来设置搜寻特定的邮箱,当所选取的邮箱越多时,理所当然每一次进行搜寻作业时所花费的时间会相对变长。

在搜寻名称与储存位置的部份,必须设置一个搜寻名称,而这个搜寻名称也将会成为之后储存在搜寻结果邮箱中的文件夹名称。接着您必须点选 [浏览] 按钮来选取前面我们所建立的探索邮箱,当然啦!您也可以在浏览窗格中选取系统默认的探索邮箱来储存搜寻结果的邮件项目。

接下来建议您也将 [搜寻完成时传送电子邮件给我] 的设置勾选,如此一来将可以在该搜寻设置完成搜寻作业时,收到一封由系统自动发送的 E-mail 通知,然后您

便可以点选 E-mail 通知属性中的超链接来开启探索邮箱。而在 [启用完整的记录] 项目设置部份, 则是可以让您取得一份完整的搜寻结果记录文件。完成以上设置之后请点选 [储存] 按钮, 系统将会开始进行第一次的邮箱探索作业。

完成了多重邮箱的搜寻作业之后, 您便可以透过 OWA 来开启探索邮箱。在此除了可以看到除了默认的收件夹项目之外, 之前所有在 ECP 域站中进行过的搜寻设置, 都会根据所设置的搜寻名称, 在这个邮箱中来建立文件夹, 展开之后可以看到所有符合搜寻条件的文件夹分类 (以被搜寻的邮箱名称分类), 这里头将会存放所有符合搜寻条件的邮件项目。值得注意的是如果所指定搜寻的用户邮箱中, 没有任何一封以上符合条件的电子邮件, 那么该文件夹是完全不会自动建立的。在搜寻记录文件部份, 在默认的状态下则同样会以 E-mail 方式寄给该探索管理者, 他所储存的文件格式将会以 CSV 档案为主, 您可以透过 Excel 程序来开启即可进行查看完成的记录属性。

使用 Exchange 命令控制台管理多重邮箱的探索

有许多 IT 人员喜好使用 Exchange 的命令控制台来管理 Exchange Server 2007, 因此请想想看针对 Exchange Server 2010 所提供的多重电子邮箱探索功能, 也一样可以透过 Exchange 的命令控制台来进行管理吗, 该怎么做呢?

有关于搜寻电子邮箱的设置与管理部份, 除了可以透过方便简单的 ECP 域站页面之外, 邮箱探索人员也可以选择透过 Exchange 命令控制台来进行管理。首先让我们来看看有关于一个建立搜寻设置的简单范例。

如图 3 所示在这个范例首先笔者下达了 Get-Mailbox 搭配 OrganizationalUnit 参数, 来指定唯一针对 Account 这个组织单位 (OU) 来应用搜寻设置。接着在管线之后的 Search-Mailbox 则是搜寻邮箱的设置命令, 整个命令语法中包括了搜寻关键词的设置 (SearchQuery)、搜寻目标邮箱的设置 (TargetMailbox)、目标文件夹的设置 (TargetFolder) 以及记录档案的层级。

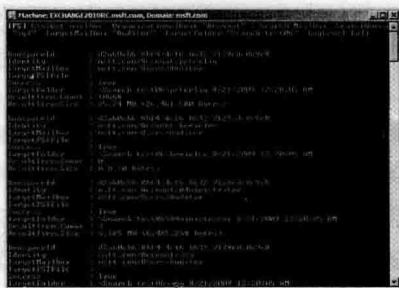


图 3 以命令方式建立搜寻

注意

请注意! 如果您像范例中一样没有使用 SourceMailboxes 参数来设置所有搜寻的邮箱, 并且没有搭配 Get-Mailbox 来设置搜寻范围, 则系统默认将会搜寻整个组织中的邮箱, 而这时候建立搜寻设置的命令也必须改成 New-MailboxSearch。

完成了以上搜寻项目的建立之后, 对于一些基本的管理工作, 一样可以透过命令方式来完成, 例如您需要修改现有的搜寻项目设置, 可以下达 Set-MailboxSearch 命令参数, 想要删除一个搜寻项目则可以下达 Remove-MailboxSearch 命令参数, 如果想要运行一个现有的搜寻设置项目, 则可以运行 Start-MailboxSearch 命令参数, 如果想要中止一个进行搜寻中的作业则可以下达 Stop-MailboxSearch 即可。

如何在 Outlook 2010 中同时开启探索邮箱

有关于多重邮箱的探索管理范例中, 都是直接使用了 Exchange Server 2010 的 OWA 来开启探索邮箱, 想想看如果想要使用 Outlook 2010 来同开启探索邮箱, 应该怎么做呢?

很简单, 只要在 Outlook 2010 联机登入自己的邮箱之后, 接着点选左上角中的下拉选单然后点选位在 [Account Settings] 下拉选单中的 [Account Settings] 继续。

紧接着将会开启 [Email Accounts] 页面, 请在 [Email] 页签中选取现有的 Exchange 账户, 然后点选 [Change] 按钮。接着会来到 [Microsoft Exchange Settings] 页面, 请点选右下角的 [More Settings] 按钮继续。接着将会开启 [Advanced] 页面, 只要点选 [Add] 按钮来将输入所要开启的探索邮箱名称即可。

设置 AD RMS 主机集成 Exchange Server 2010

相信目前有许多公司网络内,已经有部署 Windows Server 2008 所配置的 AD RMS 主机,如果进一步打算透过新配置的 Exchange Server 2010 来与它进行集成,以便可以透过传输规则来保护重要电子邮件的发送。那么,在 AD RMS 伺服端与 Exchange Server 2010 需要完成哪一些设置,才能够让两者顺利进行联机。

首先来看看有关于 AD RMS 伺服端的设置部分。请以系统管理员身份登入并开启到 AD RMS 域站文件夹的路径中,然后针对默认的 _wmcs 文件夹按下鼠标右键选择开启[属性]。请切换到[安全性]的页面中,先将 Exchange Server 2010 计算器加入到清单中,并且赋予[完全控制]权限。请接着点选[高级]按钮。

注意

请注意!在此所指定的 Exchange Server 2010 计算器对象,必须是担任集线器传输服务(Hub Transport)的计算器,因为在许多中大型的拓扑架构中(Topology),您可能会将五大角色分散部署在不同的主机上。

在[用户权限]页面中请点选[编辑]按钮继续。接下来请在[用户权限]页面中,将最下方的[以此对象的继承权限取代所有子系现有的继承权限]项目设置勾选,并且点选确定即可完成设置。如此一来便可以让 Exchange Server 2010 的主机有权限存取 Ad RMS 的域站。

如何设置 Exchange 2010 服务器的 IRM

请到 Exchange Server 2010 的命令控制台,然后输入 Set-IRMConfiguration -InternalLicensingEnabled \$true 命令参数,来启用 IRM 内部授权设置,接着您可以输入 Get-IRMConfiguration 来查看其设置是否已经成功启用。另外如果有使用到外部对于 AD RMS 的存取时,才需要将 ExternalLicensingEnable 同样设置为 True。

由于我们在前面的步骤中,已经从 AD RMS 服务器上建立了 RMS 权限策略模板了,因此紧接着您可以输入 Get-RMSTemplate 命令,来查看目前在 Exchange Server 2010 服务器上所能正确撷取到的 RMS 权限策略模板列表,其中[Do Not Forward]与[Internet

Confidential]是系统默认的模板项目,其它两个中文的策略模板则是笔者所建立。

建立集成 AD RMS 传输规则

如果目前您已经将公司的 AD RMS 主机与 Exchange Server 2010 主机完成了相关必要的集成设置,那么接下来应该怎么做才能够让重要邮件发送,自动受到 RMS 模板的保护呢?其实很容易,当您完成了所有关于 AD RMS 与 Exchange Server 2010 的集成设置之后,便可以开始设置有关于集成 AD RMS 权限策略模板,来自动应用在 E-mail 上的传输规则了。请在开启 Exchange 管理控制台(EMC)之后,切换到[Organization Configuration][Hub Transport]项目节点上,然后先点选至[Transport Rules]页签,接着点选位在[Action]窗格中的[New Transport Rule...]连结继续。

接下来会开启[New Transport Rule]精灵页面,在此可以设置将应用 RMS 权限策略模板至发送者 E-mail 的条件。举例来说,我们选择了当发生 Sales 通讯群组之间的成员在进行 E-mail 互寄时,每一封 E-mail 都会应用接下来步骤中所设置的 RMS 权限策略模板。当然啦!您可以设置针对特定的主题与属性的关键词,或是特定用户所寄送的 E-mail 等等条件的组合来作为判断的条件。接下来在[Actions]设置页面中,如图 4 所示先将[rights protect message with RMS template]项目勾选,然后点选下方窗格中相对应的超链接继续。

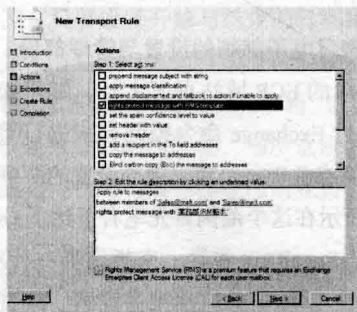


图 4 设置传输规则动作

接着便可以在此[Select RMS template]窗格中,来挑选我们前面所建立过的任何一个 RMS 权限策略模板项目进行应用。由此可见我们可以根据不同的传输规则需求,来设置不同的传输条件搭配不同的 RMS 模板。

最后在[Exceptions]页面中,如果想要设置前面动作中的排除条件,便可以在此进行设置,例如您可以设

置当 Email 是寄送业务部的某一位成员时，或是主题与属性中包含特定的关键词时，不要进行 RMS 的加密处理等等。

当完成了一项 RMS 权限策略模板的传输规则新增设置之后，便可以看见有关于这项传输规则完整的 PowerShell 命令语法，您可以将这个命令范例按下键盘上的 [Ctrl]+[C] 复制到剪贴簿中，然后张贴到任何的文书编辑器进行修改并且储存成 PS1 的扩展名格式，即可变成一个快速完成设置的手稿，往后便可以不再需要透过图形接口来进行设置了。

自我测试小秘诀

如果您想要在 Exchange 2010 伺服器端，先行测试与 RMS 集成的功能是否没问题，只要在 Exchange 命令控制台中输入 `Test-IRMConfiguration -Sender` 发送者 Email 地址，即可得知从整个 IRM 设置的加载、RMS 凭证的取得、到 RMS 模板应用的联机要求运作是否正常。

客户端电子邮件传送测试

完成了传输规则的新增之后，接下来请开启预先准备好的 Outlook 2010 客户端准备收信，然后开启 OWA 域站以不同于 Outlook 2010 联机的用户帐户来登入，并且寄送一封 E-mail 给 Outlook 2010 的用户邮箱，如此一来只要发送者与收件者符合前面的传输规则条件设置，那么收件者将会在 Outlook 2010 中收到一封 IRM 的加密邮件。

注意

请注意！当 Outlook 2010 第一次收到一封经由 RMS 加密的邮件时，将会弹出需要检查您的凭证与下载您权限的窗口，此时只要将 [Don't show this message again] 设置勾选，往后对于接收新的 RMS 加密邮件时便不会再出现此邮件。

接着当收件者开启经由传输规则的 RMS 权限策略模板，所自动加密过的 E-mail 之后，将会显示企业所设置的合规性讯息。仔细看一下，您会发现这一位收件者无法对于该封 E-mail，进行回复、回复全部以及转送等动作，全部按钮都以反白呈现而无法点击。甚至于如果想要以屏幕复制（Print Screen）的方式来撷取画面也是没有办法的。至于如果收件的用户想要查看自己针对这一封 RMS 加密邮件的权限列表，只要按下鼠标右键并点选 [检视权限] 即可得知。

结语

从本文的几个实作例子当中，不然发现 Exchange Server 2010 在企业电子邮件合规性管理能力上的强化设计，让电子邮件不仅在组织内的发送过程之中受到安全保护，即便是在与外部客户或合作伙伴之间来往的电子邮件讯息，也同样可以得到同等级的安全保护机制，让许多商业机密的讯息内容，不会因此遭到恶人士的窃取、伪造以及窜改，让企业电子商务的往来风险降至最低。



FCoE 在 Linux 下的部署

大庆 栗朝军

FCoE (Fibre Channel over Ethernet) 以太网光纤通道的出现，解决了 LAN 和 SAN 的融合问题，FCoE 技术标准可以将光纤通道映射到以太网，可以将光纤通道信息插入以太网信息包内，从而让服务器-SAN 存储设

备的光纤通道请求和数据可以通过以太网连接来传输，而无需专门的光纤通道结构。

FCoE 的部署

FCoE 可以只部署在服务器网络接入层。目的是实现服务器 I/O 整合, 简化服务器网络接入层的线缆设施。服务器安装支持 FCoE 的网卡, 并连接到接入层 FCoE 交换机, 接入层交换机再分别通过 10GE 链路和 FC 链路连接到现有的 LAN 和 SAN; FCoE 也可以整网端到端(接入—汇聚—核心)部署。FCoE 技术的应用范围扩大到整网, 除接入层交换机外, 汇聚核心层交换机也支持 FCoE 功能; 除服务器外, 存储设备也需支持 FCoE 接口。由此实现了 LAN 与 SAN 的融合, 简化了整网基础设施。虽然目前原生支持 FCoE 的存储设备很少, 但除了连接原生 FCoE 存储设备外, 用户仍可通过 DCB/CEE 交换机与 FC 交换机连接, 让 FCoE 服务器端存取传统的 FC 存储设备, 且能沿用原有的 FC 管理模式。

在 FCoE 的服务器端, 适配卡可以有三种选择。

1) 聚合网络适配卡(CNA)。CNA 卡大都属于 Emulex、Qlogic、Brocade 等传统光纤通道厂商的产品, 拥有完整的硬件卸载(Offload)引擎, 既可处理封装在 TCP/IP 协议封包, 也可处理 FCoE 帧(封装了 FCP 封包的以太网帧)。CNA 卡的运用更具弹性, 而且凭借完整的硬件卸载引擎, 耗用的主机运算资源相对较少。

2) 具有 FCoE 硬件卸载引擎的 10Gb 以太网卡。这类网卡是由传统的 NIC 厂商推出, 具有不同程度的 FCoE 卸载功能, 可以减轻主机处理 FCoE 的运算负担, 但卸载功能不如 CNA 卡那样完整, 仍须配合 Initiator 软件支持。

3) 一般的 10Gb 以太网卡。仅具备一般 LAN 网络传输用的 TCP 卸载引擎, 但不具备 FCoE 卸载功能, 相关运算工作必须通过 Initiator 软件交由主机承担。

FCoE 适配卡在 Linux 下配置

在 Linux 下使用使用不完全 FCoE 硬件卸载功能 FCoE 适配器主要用到三个组件: lldpad、dcbttool 和 fcoeadm, 而具有完全的 FCoE 硬件卸载功能 CNA 卡主要使用 fcoeadm 配置工具。

下面针对具有完整 FCoE 硬件卸载功能和部分卸载功能的网卡的使用分别加以说明:

1、聚合网络适配卡(CNA)使用与配置

下面以 Broadcom 的 CNA 卡, 操作系统为 RHEL 6.4 为例, 介绍聚合网络适配卡(CNA)使用与配置(所有

操作需要 root 用户权限):

1) 在服务器 PCIe 插槽正确安装 CNA 卡, 并确保 CNA 卡 BIOS 中启用 FCoE 完全卸载功能。安装 Broadcom 的 Red Hat Enterprise Linux 6 的多功能驱动程序。

2) 在控制台使用 ethtool 命令识别出驱动好的网卡, 本例中是 eth2, 其命令形式为:

```
#ethtool eth2
```

该命令会显示网卡的速率、端口类型等信息。

3) 安装 FCoE 相关工具包, 如果在安装操作系统时没有安装, 可以在 Redhat 安装介质的 packages 文件夹中找到并手动安装, 在 RHEL 6.4 及以下, 包的名字是 fcoe, 在 RHEL 6.5 中变为 fcoe-util, 同时找到 lldpad(链路层发现协议代理守护程序), 使用 rpm 命令手动安装。

4) 创建该网络适配器的 FCoE 配置文件

```
#cp /etc/fcoe/cfg-ethx /etc/fcoe/cfg-eth2
```

将默认的 FCoE 配置文件复制到 /etc/fcoe/cfg-eth2。这里网卡是处理 FCoE 的网卡, 其编号会根据具体情况有所不同。

5) 修改文件 /etc/fcoe/cfg-eth2 中 "DCB_REQUIRED" 为 "NO"。由于 CNA 卡拥有完整的硬件卸载(Offload)引擎, 不需要 DCB 服务, 因而需要手动禁止。

如果需要启动时自动加载可以在相应配置文件, 在相应配置文件中修改 "ONBOOT=yes" 本例中的配置文件为 /etc/sysconfig/network-scripts/ifcfg-eth2。配置好 IP 和掩码等信息, 当然这一步骤工作也可以通过终端和 GUI 下配置工具完成而无需手工修改配置文件。

6) 手动禁止 CNA 接口上的 lldpad 守护进程

```
#lldptool set-lldp -i eth2 adminStatus=disabled
```

由于 CNA 卡拥有完整的硬件卸载(Offload)引擎, 需要把 Broadcom CNA 卡上的 lldpd 关闭, 以让其使用 Broadcom 的 FCoE offload。

7) 确保 /var/lib/lldpad/lldpad.conf 文件中对应 eth2 的 "adminStatus" 设置为 "0"。

8) 启动 LLDP 服务和 FCoE

```
#service lldpad restart
```

```
#service fcoe restart
```

使用 chkconfig 命令使 lldpad 和 FCoE 两个服务配置为启动时就自动开启

```
#chkconfig lldpad on
```

```
#chkconfig fcoe on
```

9) 验证所有 FCoE 连接


```
#fcoeadm -i
```

10) 设置 FCoE 发起程序磁盘的分区, 磁盘上创建文件系统

使用 fdisk 命令为 FCoE 发起程序磁盘设置分区。

```
#fdisk /dev/sdc
```

使用 mkfs 命令在 FCoE 发起程序磁盘上创建文件系统。

```
#mkfs /dev/sdc
```

2、FCoE 硬件卸载引擎的 10Gb 以太网卡配置与使用

下面以 RHEL 6.4 和 Intel Ethernet Converged Network Adapter X520 系列网卡为例, 说明具有 FCoE 硬件卸载引擎的 10Gb 以太网卡配置与使用。

1) 验证网卡驱动。以 root 用户的身份登录服务器。RHEL 6 中已经包含了大部分 10Gb 以太网卡驱动, Intel 82599 10GbE 网络控制芯片已经可以直接内置驱动, 在控制台使用 ethtool 命令识别网卡, 本例中是 eth2, 其命令形式为:

```
#ethtool eth2
```

该命令会显示网卡的速率、端口类型等信息。

2) 安装 FCoE 相关工具包, 如果在安装操作系统是没有安装, 可以在 Redhat 安装介质的 packages 文件夹中找到手动安装, 在 RHEL 6.4 及以下, 包的名字是 fcoe, 在 RHEL 6.5 中变为 fcoe-util, 同时找到 lldpad (链路层发现协议代理守护程序), 使用 rpm 命令手动安装。

3) 将默认的 FCoE 配置文件复制到 /etc/fcoe/cfg-eth2。

```
#cp /etc/fcoe/cfg-ethx /etc/fcoe/cfg-eth2
```

同时脚本里有一些重要配置选项需要加以确认:

```
fcoe_enable=yes // 指示该端口运行 FCoE 服务
```

```
dcb_required=yes // 指示该端口需要 DCB 服务
```

```
auto_vlan=yes // 指示 fcoemon 处理被发现的
```

VLAN 信息

4) 如果需要启动时自动加载可以在相应配置文件, 在相应配置文件中修改 "ONBOOT=yes" 本例中的配置文件为 /etc/sysconfig/network-scripts/ifcfg-eth2. 配置好 IP 和掩码等信息,

```
ONBOOT=yes // 启动时自动加载配置
```

当然这一步骤工作也可以通过终端和 GUI 下配置工具完成而无需手工修改配置文件。

5) 使用 chkconfig 命令使 lldpad 和 FCoE 两个服务配置为启动时就自动开启

```
#chkconfig lldpad on
```

```
# chkconfig fcoe on
```

启动服务:

```
#service fcoe start
```

开启 LLDP 服务, 因为 DCBX 协商需要 LLDP 协议的支持, 有些网卡会因为 DCBX 协商失败, 就无法进行 FCoE 登录。

```
#service lldpd start
```

6) 用 dcbtool sc 命令在指定的 FCoE CNA 卡上启用数据中心桥接,。

```
#dcbtool sc eth2 dcb on
```

系统将返回类似以下信息:

```
Version: 2
```

```
Command: Set Config
```

```
Feature: DCB State
```

```
Port: eth2
```

```
Status: Successful
```

7) 在指定的 FCoE 适配卡启用数据中心桥接, 以接受交换机的 FCoE 优先级设置。

```
#dcbtool sc eth2 app:0 e:1
```

系统将返回类似以下信息:

```
Version: 2
```

```
Command: Set Config
```

```
Feature: Application FCoE
```

```
Port: eth2
```

```
Status: Successful
```

"app" 子类型参数可以是 0 或 fcoe, 其他的可选子类型如下:

```
0: fcoe - Fiber Channel over Ethernet ( FCoE )
```

```
1: iscsi - Internet Small Computer System Interface ( iSCSI )
```

```
2: fip-FCoE Initialization Protocol ( FIP )
```

8) (可选) 启用并设置数据中心桥接的优先级流量控制 (PFC) 设置。

```
#dcbtool sc eth<x> pfc e:1 a:1 w:1
```

自变量设置值为: e:<0|1>

控制功能启用, a:<0|1> 控制是否通过数据中心桥接交换协议向对等体推广功能。

w:<0|1> 控制功能是否希望根据从对等体接收到的反馈来更改其操作配置。

9) 验证配置。可以用如下命令验证配置是否正确:

```
# dcbtool go eth2 pfc
```


系统将返回类似以下信息：

```
Version: 2
Command: Get Oper
Feature: Priority Flow Control
Port: eth2
Status: Successful
Oper Version: 0
Max Version: 0
Errors: 0x00 - none
Oper Mode: true
Syncd: true
pfcup: 0 0 0 1 0 0 0 0
#dcbtool go eth2 app:fcoe
```

系统将返回类似以下信息：

```
Version: 2
Command: Get Oper
Feature: Application FCoE
Port: eth2
Status: Successful
Oper Version: 0
Max Version: 0
Errors: 0x00 - none
Oper Mode: true
Syncd: true
```

9) 重启 FCOE、lldp 服务 并验证

```
#service fcoe restart
#service lldpd restart
```

在验证交换机和存储配置前，进行验证以确认 FCoE 服务运行。注意：当使用创建了 VLAN 标记 Intel 网卡时，它会读到和使用交换机上的 FCoE VLAN(110)。

```
#service fcoe status
```

系统将返回类似以下信息：

```
11786
/usr/sbin/fcoemon --RUNNING, pid=11786
Created interface: eth2.110-fcoe
```

检查 FCOE 状态，检查 FCOE 状态主要使用 fcoeadm 工具，fcoeadm 实用程序通过套接字接口将命令发送给正在运行的 fcoemon 进程。其它功能请参见 fcoemon 手册页。

查看 FCoE 发起程序状态以获取 FC-ID 节点 / 端口号：

```
#fcoeadm -i eth2.110
```

系统将返回类似以下信息：

```
Description: 82599EB 10-Gigabit SFI/SFP+
Network Connection
Revision: 01
Manufacturer: Intel Corporation
Serial Number: 001B219B258C
Driver: ixgbe 3.3.8-k2
Number of Ports: 1
Symbolic Name: fcoe v0.1 over eth2.110
OS Device Name: host8
Node Name: 0x1000001B219B258E
Port Name: 0x2000001B219B258E
FabricName: 0x2001000573D38141
Speed: 10 Gbit
Supported Speed: 10 Gbit
MaxFrameSize: 2112
FC-ID( Port ID ) : 0x790003
State: Online
```

在这里可以看到 WWN 信息和状态信息，WWN 信息会在设置存储设备时用到。通过 lldptool -tni eth2 可以查询到接收的交换机端口信息，包括交换机名和端口信息等：

```
#lldptool -tni eth2
```

系统将返回类似以下信息：

```
Chassis ID TLV
MAC: 54:77:ee:c1:74 :66
Port ID TLV Local:Eth1/9
Time to Live TLV
120
Port Description TLV
Ethernet 1/9
System Name TLV
DC-Net5010-1
```

查看 FCoE 目标以获取 FC-ID 节点 / 端口号：

```
#fcoeadm -t eth2.110
```

系统将返回类似以下信息：

```
Interface: eth2.110
Roles: FCP Target
Node Name: 0x200000D0231B5C72
Port Name: 0x210000D0231B5C72
Target ID: 0
MaxFrameSize: 2048
```

OS Device Name: rport-8:0-7

FC-ID (Port ID): 0x79000C

State: Online

LUN ID	Device Name	Capacity	Block Size	Description
40	/dev/sdg	100.00 GB	512 IFT DS S24F-R2840-4 (rev 386C)	

11) 设置 FCoE 发起程序磁盘的分区, 磁盘上创建文件系统。使用 fdisk 命令为 FCoE 发起程序磁盘设置分区, 用 mkfs 命令在 FCoE 发起程序磁盘上创建文件系统。

```
#fdisk /dev/sdg
```

```
#mkfs /dev/sdg
```

这样 REDHAT 下 FCOE 配置就完成了。这里要注意的是以上配置是 OPEN-FCOE 提供的。CNA 网卡产商也会提供相应的 FCOE 查看工具。

FCoE 交换机配置

虽然 FCoE 的物理层采用了 10Gb 以太网, 但它实现上是基于 CEE (Convergence Enhanced Ethernet) / DCB (Data Center Bridging) 增强型以太网, 而非一般 IEEE 802.3ae 10Gb 以太网。要解析封装在 FCoE 中的光纤通道协议 (FCP) 封包, 仍须通过可支持 FCoE 的网络设备, 而不能使用一般 10GbE 网络设备。在网络端, 必须搭配支持 FCoE 与 CEE/DCB 的 10Gb 交换机, 如 Brocade 的 8000 系列交换机、Cisco 的 Nexus 5000 系列交换机, H3C 12000 系列等。

交换机的 FCoE 端口上承载三类 VLAN: 服务器 VLAN (承载普通以太网报文)、存储 VLAN (承载 FCoE 数据报文)、FIP VLAN (承载 FCoE 初始化协议报文)。服务器到 FCoE 交换机的报文中, FCoE 数据报文采用 TAG 方式, FIP 报文和普通以太网报文采用 UNTAG 方式。FCoE 数据报文对应的 VLAN ID, 由 FIP 协议与 FCoE 交换机协商获得。在部署时, 应将交换机的 FCoE 端口配置成 Hybrid 类型, 允许存储 VLAN 报文以 TAG 方式通过, 服务器 VLAN 报文和 FIP 报文以 UNTAG 方式通过, 并将该端口的 PVID 设置为服务器 VLAN 的 VID。当该端口收到除 FIP 协议以外的其它 UNTAG 报文时, 将在服务器 VLAN 内转发该报文。这里将 FIP VLAN 配置成“协议 VLAN 模式”, 是为保证服务器在获取存储 VLAN 的 VID 前, FIP 协议能够通过

“协议 VLAN”完成 FCoE 初始化过程。接入层 FCoE 交换机在正常转发时, 来自服务器的 FCoE 数据报文, 通过存储 VLAN (TAG 方式) 转发到交换机 FC 端口上行到 FC SAN。而来自服务器的普通以太网报文则按正常流程转发, 就接入层 FCoE 交换机而言, 主要功能是将服务器端接收的报文进行 LAN 业务与 SAN 业务分离。

对于 Cisco Nexus 5000 系列交换机平台, 需要把虚拟的 vfc 端口绑定到特定以太网端口是实现 FC 转发。其配置样例如下:

```
Configure
```

```
feature fcoe // 全局开启 fcoe 功能
```

```
vlan 3 //vlan3 关联 vsan 3
```

```
fcoe vsan 3
```

```
interface vfc3 // 创建 vfc3 虚拟接口, 这个端口与服务器端的 CNA 网卡相连
```

```
bind interface Ethernet1/3 // 绑定物理接口, 同时 no shutdown 接口
```

```
no shutdown
```

```
interface vfc7
```

```
bind interface Ethernet1/7 // 创建 vfc3 虚拟接口, 这个端口与存储端的 CNA 网卡相连
```

```
no shutdown
```

```
vsan database // 在 vsan 数据库中将相应的 vfc 接口关联到 vsan3 中, 这里要注意服务器要获取到存储分配的 lun, 就需要把存储的接口也关联到这个 vsan 下。
```

```
vsan 3 interface vfc3
```

```
vsan 3 interface vfc7
```

```
interface Ethernet1/3 // 物理接口配置成 trunk 模式, switchport mode trunk
```

```
spanning-tree port type edge trunk
```

```
interface Ethernet1/7
```

```
switchport mode trunk
```

```
spanning-tree port type edge trunk
```

```
zone default-zone permit vsan 3 // 划分 zone 信息, vsan3 内的信息要转发就需要划到相应的 zone 中。
```

通过 sh fcns database detail 命令, 在表项中可以看到 CNA 网卡的具体产商和一些注册信息。当然对于更为复杂的拓扑结构, 还需要进一步配置, 上述样例仅提供了最基本的配置思路, 在实践中更细节的配置请参见交换机的说明文档。

◆ 日志审计分析系统的应用

▼ 武汉 李懿

数据中心作为企业信息化建设中的核心,由大量网络设备、安全设备、操作系统、应用服务等组成,管理员要对所管理的各种设备进行巡检,以及时发现问题,但面对海量的日志数据,如何进行有效处理,成为管理员所面对的问题。

日志审计分析系统(下简称日志系统)作为统一的日志收集与分析平台,在数据中心的作用既有日常管理作用,也有安全审计作用。日志系统通过对数据中心网络设备、安全设备、服务器、应用系统日志进行全面的标准化收集和存储,为管理员提供了集中的日志查看、检查平台,通过日志系统的关联、分析、告警功能,帮助管理员第一时间了解各类安全事件,通过各类报表、查询功能,为管理员提供合法合规、内控要求的报表。

日志系统可以方便的部署到现有数据中心网络环境中,只要网络能够到达平台即可实现日志的收集,但由于需要获取相关网络流量日志,建议一般连接在核心交换机上。

日志系统日志采集方式主要有安装代理方式,主要在操作系统内安装代理程序,与管理平台相关联,将系统日志发送给管理平台。

syslog 方式,适用于网络设备及安全设备,在设备中启用 syslog 进程,将管理平台地址设置为日志发送地址;端口镜像方式,在网络设备配置流量镜像端口,与管理平台相连,在管理平台上进行端口过滤,得到诸如数据库、web 访问等的流量数据,从而形成相应日志信息;文件采集方式,可定时将文本型日志采集到管理平台进行存储分析。

日志系统在对海量日志收集后,用户需要平台自带的关联分析功能、规则定义功能、日志报表的定义,来实现管理员对日志分析的要求。以下从几个不同日志类型来了解:

数据库日志

一般来说有两种,一种是通过字段收集直接发送给日志系统,另一种日志系统通过流量端口过滤主动抓取。不管是哪种收集日志方式,日志系统通过自身的关联分析引擎,能够产生一段时间内用户对数据库操作的语句记录,或者产生一段时间内用户登录数据库的登陆记录,管理员通过查看这些信息检查数据库是否存在健康或安全问题,如图 1 所示。

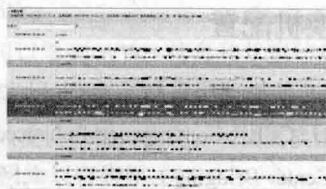


图 1 数据库操作记录

操作系统日志

一般来说,通过在操作系统内安装代理程序,将操作系统产生的事件日志直接发送给管理平台。这种日志首先需要管理员在操作系统中进行启用配置,默认情况下,Windows 操作系统安全策略审核日志是不开启的,需要手工配置,以保证所需要的日志能产生,其次需要管理员明确所关注的事件及相应事件项,比如系统的开关机、登陆的成功或失败、磁盘问题等,这些在日志系统中基本都有内置规则,管理员也可根据自己需求自定义规则,如图 2 和图 3 所示。

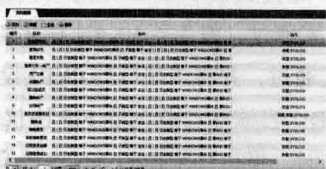


图 2 审核日志

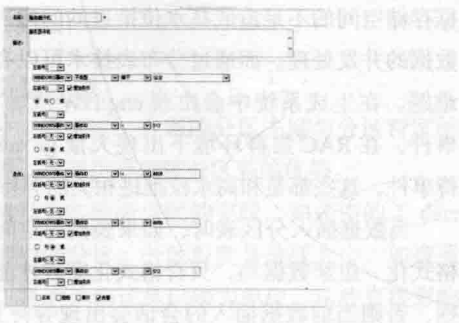


图 3 定义日志规则

自定义或使用内置报表，生成报表后供管理员使用，如图 4 所示。

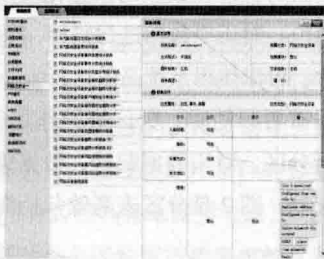


图 4 关心设备状态性能

网络及安全设备日志

此类日志是通过启用 syslog 进程，将设备日志发送到日志系统。

对此类设备，管理员通常会关心设备状态、性能等，那么对于该类日志分析，建议管理员收集日志关键字，

上述三种类型的日志为比较常用的日志，涉及到了日志平台的关联引擎、内置规则、报表定义等方式。

管理员在使用时可以灵活使用，还可以利用日志系统短信、邮件功能发送所关注的日志，使管理员能利用日志平台及时了解数据中心内系统、应用状态，提高对数据中心服务故障的响应。

如何使用 Oracle 数据库分区表

北京 殷圣忠

Oracle 作为一种数据库，处理海量数据最基本的方法就是“分而治之”，即将海量表拆成小表，具体技术而言就是采用分区表的形式拆分大表，从而提高用户在海量数据环境下的用户体验，减少 DBA 维护的时间和精力成本从而有效降低海量数据处理的复杂度。

分区表与海量数据

海量数据的特点是在高并发环境下的高数据量，这样就造成传统的单表（具有单独的段标识）很大。如此大的数据量，极有可能引起数据访问以及管理的各种问题。

Oracle 解决这种海量数据的方法是利用分区表技术。所谓的分区表就是依据分区主键而创建的多个独立的表。对应用而言它只是一个表，而在底层是由几个独立分区组成，每个分区具有自己的段标识以及段的高水位

线。图 1 是按照时间分区的分区表示意图。从图 1 可以看出，分区表在物理上是独立的存储段，其优点是：其一，数据分布到多个独立的段中，单个段的损坏不影响其他段的数据，提高了段的可用性；其二，对每个分区实施单独的备份和恢复策略，提供了段管理的灵活性；其三，不同的物理分区可以存储到不同的物理磁盘上从而来分散 I/O，提高了数据 I/O 性能。



图 1 分区表示意图

分区表与数据归档

对历史数据的备份在成熟的信息化应用系统中占有十分重要的地位。对历史数据进行归档,降低其数据量,消除磁盘碎片,可以使得系统高效运行。

在有数据需要归档时,分区表的作用就发挥出来,按照时间进行分区,对于数据归档,数据维护,数据的可用性都有好处。图 2 是分区表高效归档海量数据示意图。

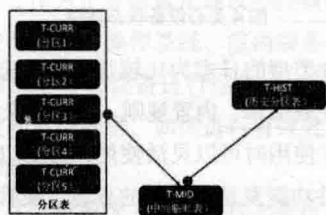


图 2 高效归档海量数据分区表示意图

在生产实际中,经常需要按照时间进行历史数据归档,随着数据量的快速增长,需要归档这些历史数据,如果此时采用了时间分区,前提是该表有时间字段作为分区主键,就很容易使用分区技术快速高效地实现数据归档。如当前表为 T-CURR 是按照表中 T-date 字段的分区表,每个月一个分区,可按照如下步骤实现数据归档:先创建中间临时表 T-MID。然后创建历史分区表 T-HIST。最后进行分区交换。

这里的历史表 T-HIST 和当前的表 T-CURR 结构相同,唯一区别就是名称不同。而中间临时表 T-MID 与需要交换的分区具有相同的表结构。下面是具体的交换过程:

```
Alter table T-CURR exchange partition d1 with table T-MID including indexes;
```

```
Alter table T-HIST exchange partition d1 with table T-MID including indexes without validation;
```

这样通过两次分区交换完成当前表中分区 d1 中的数据归档,此时使用 including indexes 包含索引段的交换,如果是本地索引则不需要重建历史归档表中的本地索引,这里的 without validation 指出不需要数据验证,这样就不需要在交换前对 T-MID 中的数据进行全表扫描,提高分区交换的效率。

分区表解决高水位推进问题

海量数据环境下,高并发量的数据对单表而言会数

据存储空间和不足造成高水位推进的问题,从而影响到数据的并发处理。而通过分布表技术可以有效化解这个难题。在生成系统中会出现 enq:HW 或者 enq:FB 等待事件,在 RAC 集群环境下出现大量 gc current grant 等待事件,这些都是和高水位推进相关的等待事件。

当数据插入分区表时,如果表段的空间不足会首先格式化一组新数据块,只有格式化完成才能继续插入数据,否则当前数据插入的会话会出现等待 HW/FB 锁的等待。

可以想象在海量数据环境下,高并发量、高数据量的特点必然因为这种等待的加剧,从而影响数据插入的性能。此时如果合理使用分区表即可有效缓解这种等待。一旦将表分区,则每个分区具有独立的段标识,对应独立的高水位线管理。这样就将数据插入均衡到多个分区中,从而有效缓解 HW 锁的争用。

分区表与 RAC 集群环境

在 RAC 集群环境下,有效提高了数据的高可用性、可扩展性、负载均衡等,提高了系统处理海量数据的能力。结合集群环境的实际,需要考虑如何有效使用好分区表。合理的分区表使用可以减少实例间的数据争用。减少节点之间的网络流量,从而优化整个集群系统的性能。

如果条件允许,采用应用分区是十分有效的较少集群实例间数据流量的方法,它可以极大减少表的 global buffer busy 等待。即将每个区域的用户绑定到服务器连接池组中的某个固定的实例,固定的实例只用来访问一个固定区域用户的分区,这样就极大减少了实例对相同数据块的争用,从而避免 global buffer busy 带来的争用问题。

如果条件不允许使用应用分区,则需要详细分区访问该海量表的 SQL 语句特点,从而设计对应的分区方案。如果 SQL 的谓词中大量的出现某个字段的 = 条件,则可以选择该字段作为 HASH 分区的主键,从而尽最大可能将数据打散,这样通过将数据打散到不同的分区中,从而有效减少热块冲突的概率,提高整个集群的性能。

如何实施分区

1 选择分区主键

在使用分区技术时,合理的分区主键与分区粒度的选择十分重要,否则很难发挥分区表的优势。

分区主键是指实现表分区的字段,如表中的 T_date 字段实现按照时间分区。分区粒度是分区大小,如按照时间分区是以月为单位还是以年为单位,这些直接影响分区优势的发挥。

总之在设计分区前要根据业务需要,制定满足性能、维护等需求的分区方案,选择好分区主键与分区粒度。

分区主键的选择主要考虑分区目的。如果是归档数据显然使用时间字段实现范围分区;如果主要是打散数据分解全局数据冲突可以考虑谓词中的对应字段作为分区主键。即分区主键的选择原则是它是否经常出现在查询语句的谓词条件中。

如果在系统上线之后实现分区,此时 DBA 不清楚那些 SQL 经常访问,以及如何访问这些海量表,所以需要不断的分区共享池中的 SQL 语句,分区过滤条件和连接条件,从而合理判断分区主键。在选择了分区主键之后,必须保证该字段是非空的。

2 选择分区粒度

在确定了分区主键之后,就需要考虑分区粒度的选择。而分区粒度的选择没有固定的原则,适合系统需要

就好,更好的服务于应用系统就是好的分区,但是这也是分区粒度的难点。不同目的采用不同分区方法。以下列举三个目的作为说明:

(1) 便于维护:需要考虑多大的分区维护起来方便,满足维护时间窗口的条件,如果分区归档要求 15 分钟完成,则显然对分区粒度的大小有限制,这需要做实验分区,从而满足自己系统软硬件条件的容量限制。

(2) 便于归档:归档频率需要考虑,即多久归档一次,显然归档周期就是分区粒度需要考虑的首要因素

(3) 便于提高性能:需要考虑表的范围扫描的范围高概率发生在哪个时间范围内,这样根据多数数据查询的扫描时间范围设计分区粒度比较好。

结语

本文分析了如何在高并发量以及高数据量的环境下提高数据访问性能。Oracle 数据库通过分区表技术可以有效解决这个难题。

分区技术的使用需要针对具体场合以及结合分区表的特点作出合理的分区粒度以及分区键的选择。在 RAC 集群环境下合理使用应用分区可以极大减少实例之间数据通信以及实例间协商的开销,从而提高 RAC 的整体性能。



搭建 Hadoop 实验平台

广州 淡武强

实验材料

- 1、VMware Workstation ;
- 2、ubuntu14.04.3 桌面版 64 位操作系统
- 3、jdk8u 65 64 位
- 4、hadoop2.7.1

实验过程

用 VMware Workstation 创建 4 台 ubuntu 虚拟机

Windows 平台下安装好 VMware Workstation 虚拟机软件。从 ubuntu 官方网站 www.ubuntu.com 下载 ubuntu14.04.3 桌面版 64 位操作系统,通过 VMware Workstation 创建一台 ubuntu 虚拟机。用户名 hadoop, 口令 hadoop, 如图 1 所示。

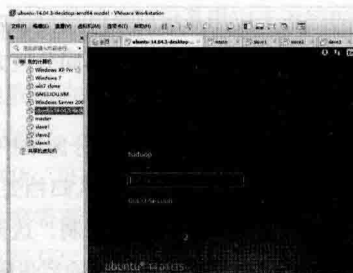


图 1 创建 ubuntu 虚拟机

安装 jdk 和 hadoop，并配置环境变量

1、安装 jdk 和 hadoop：

创建 jdk 和 hadoop 安装目录 /usr/soft：sudo mkdir /usr/soft

更改目录权限为所有用户可写入：sudo chmod a+w soft

将已下载的 jdk 和 hadoop 放入该目录下

解压缩：tar xzf jdk-8u65-linux-x64.gz

tar xzf hadoop-2.7.1.tar.gz

解压后，如图 2 所示。



图 2 安装 jdk 和 ubuntu

2、配置 jdk 的环境变量

编辑 envrin ment 文件：sudo gedit /etc/environment

添加 JAVA_HOME 环境变量：JAVA_HOME=/usr/soft/jdk1.8.0_65

在系统路径 PATH 中添加 PATH=" :usr/soft/jdk1.8.0_65/bin"

让环境变量立即生效 source /etc/environment

测试环境变量是否设置成功：

echo \$JAVA_HOME echo \$PATH

测试 jdk 安装是否成功：java version，如图 3 所示，则表示 jdk 安装成功。

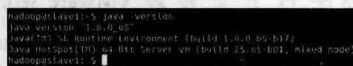


图 3 测试 jdk 安装是否成功

3、配置 hadoop 的环境量

编辑 envrinment 文件：sudo gedit /etc/environment

加入自定义环境变量 HADOOP_INSTALL

HADOOP_INSTALL=/usr/soft/hadoop-2.7.1

PATH 添加 /usr/soft/hadoop-2.7.1/bin 和 /usr/soft/hadoop-2.7.1/sbin

重启 Ubuntu，使 hadoop 环境变量生效，使用以下命令验证 hadoop 环境是否生效：

hadoop version

如果显示如图 4 所示，则表示 hadoop 安装成功。



图 4 测试 hadoop 安装是否成功

以该虚拟机为模板，克隆出 3 台虚拟机

Hadoop 集群各节点信息如下：

主机名：master

IP：192.168.189.134

角色：ResourceManager & NameNode

主机名：slave1

IP：192.168.189.130

角色：DataNode& Node Manager

主机名：slave2

IP：192.168.189.131

角色：DataNode& Node Manager

主机名；slave3

IP：192.168.189.132

角色：SecondaryName Node

Hadoop 中任一节点均可担任多种不同角色，非常灵活，本实验中的角色分配只是其中一种方式。

修改 4 台 ubuntu 虚拟机的主机名：sudo vim /etc/hostname，hostname 均为 hadoop。

修改 hosts 文件，解析主机名：sudo vim /etc/hosts

hosts 文件内容如图 5 所示。

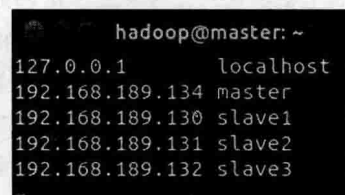


图 5 hosts 文件内容

重启虚拟机后主机名和 hosts 解析生效。

配置 SSH 无密钥登录

在 4 台虚拟机上，安装 openssh-server 安全连接软

件

```
sudo apt-get install openssh-server
```

4 台上均生成密钥对：ssh-keygen -t rsa，其位于家目录下的隐藏目录 ~/.ssh

在 master 上新建 authorized_keys 认证文件：touch authorized_keys

将 slave1、slave2、slave3 上 ~/.ssh/id_rsa.pub 公钥拷贝到 master 上

```
scp hadoop@slave1: ~/.ssh/id_rsa.pub ~/.ssh/slave1.pub
```

```
scp hadoop@slave1: ~/.ssh/id_rsa.pub ~/.ssh/slave1.pub
```

```
scp hadoop@slave1: ~/.ssh/id_rsa.pub ~/.ssh/slave1.pub
```

将 4 台虚拟机的公钥放入 authorized_keys

```
cat id_rsa.pub>authorized_keys
```

```
cat slave1.pub>>authorized_keys
```

```
cat slave2.pub>>authorized_keys
```

```
cat slave3.pub>>authorized_keys
```

如此，authorized_keys 中就有了 4 台主机的认证文件，将 authorized_keys 分发到 slave1、slave2、slave3 上

```
scp ~/.ssh/authorized_keys hadoop@slave1:~/.ssh
```

```
scp ~/.ssh/authorized_keys hadoop@slave2:~/.ssh
```

```
scp ~/.ssh/authorized_keys hadoop@slave3:~/.ssh
```

在 master 上 ssh 连接 slave1 主机：ssh slave1

首次 ssh 远程登录需输入 slave1 主机的口令，以后就可免口令登录

exit 命令退出远程登录，返回本机命令行界面

4 台主机互测均成功。

修改 core-site.xml、hdfs-site.xml、mapred-site.xml、yarn-site.xml 及 slaves，为 4 台虚拟机分配不同角色，以组成 hadoop 完全分布式集群

4 个文件位于 /usr/soft/hadoop-2.7.1/etc/hadoop/ 目录下

由于每 4 台主机的 xml 文件配置必须相同，所以只需在 master 主机上修改这 4 个 xml 文件，然后远程拷贝到其余 3 台主机即可。

注意

特别说明：默认的 hadoop 集群启动临时文件存放在 /tmp/ 目录下，每次重新开机就会被清空，与此同时 namenode 的格式化信息就会丢失。为避免 hadoop 集群启动时出现 namenode 进程丢失故障，需在 master 主机上建立一个永久的临时文件存放目录：mkdir /home/hadoop/hadoop_tmp。

同时打开所有的 xml 文件：gedit *.site.xml。

1、core-site.xml 用于配置 namenode 节点，修改后内容为

```
<?xml version="1.0" encoding="UTF-8"?>
```

```
<?xml-stylesheet type="text/xsl" href="configuration.xsl"?>
```

```
<configuration>      <!--Configurations for
NameNode ( Secondary NameNode ), DataNode、
NodeManager:-->
```

```
<property>      <name>fs.defaultFS</name>
```

```
<value>hdfs://master:9000</value>
```

```
<description>NameNode URI</description>
```

```
</property>
```

```
<property>
```

```
<name>hadoop.tmp.dir</name>
```

```
<value>/home/hadoop/hadoop_tmp</value>
```

```
<description>A base for other temporary directories.</description>
```

```
</property>
```

```
</configuration>
```

2、hdfs-site.xml 用于配置 secondary namenode 节点，修改后内容为

```
<?xml version="1.0" encoding="UTF-8"?>
```

```
<?xml-stylesheet type="text/xsl" href="configuration.xsl"?>
```

```
<configuration>
```

```
<!--Configurations for NameNode:-->
```

```
<property>
```

```
<name>dfs.namenode.secondary.http-address</name>
```

```
<value>slave3:50090</value>
```

```
</property>
```

```
<property>
```

```
<name>dfs.replication</name>
```

```
<value>2</value>
```



```
</property>
</configuration>
```

3、mapred-site.xml 需从 mapred-site.xml.template 模板复制而来，修改后内容为

```
<?xml version=" 1.0"?>
<?xml-stylesheet type="text/xsl" href="configuration.
xsl"?>
```

```
<configuration>
<property>
<name>mapreduce.framework.name</name>
<value>yarn</value>
</property>
</configuration>
```

4、yarn-site.xml 用于配置 resourcemanager，本实验中 resourcemanager 由 namenode 节点兼任，修改后内容为

```
<?xml version=" 1.0"?>
<configuration>
<property>
<name>yarn.resource manager.hostname</name>
<value>master</value>
</property>
<property>
<name>yarn.resource manager.address</name>
<value>master:8032</value>
<description> ResourceManager host:port for clients to
submit jobs.NOTES:host:port If set, overrides the hostname
set in yarn.resourcemanager.hostname.</description>
</property>
<property>
<name>yarn.resource manager.scheduler.address</
name>
<value>master:8030</value>
<description> Resource Manager host:port for
ApplicationMasters to talk to Scheduler to obtain resources.
NOTES:host:port If set, overrides the hostname set in yarn.
resourcemanager.hostname</description>
</property>
<property>
<name>yarn.resourcemanager.resource-tracker.
address</name> <value>master:8031</value>
<description>Resource Manager host:port
```

for NodeManagers.NOTES:host:port If set, overrides the hostname set in yarn.resourcemanager.hostname</description>

```
</property>
<property>
<name>yarn.resourcemanager.admin.address</name>
<value>master:8033</value>
<description> Resource Manager host:port for
administrative commands.NOTES:host:port If set, overrides
the hostname set in yarn.resourcemanager.hostname.</
description>
```

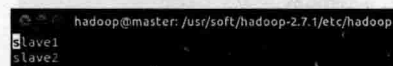
```
</property>
<property>
<name>yarn.resourcemanager.webapp.address</name>
<value>master:8088</value>
<description> ResourceManager web-ui host:port.
NOTES:host:port If set, overrides the hostname set in yarn.
resourcemanager.hostname</description>
```

```
</property>
<property>
<name>yarn.node manager.aux-services</name>
<value>mapreduce_shuffle</value>
</property>
</configuration>
```

将上述 4 个 xml 文件从 master 上 copy 到其它 3 个节点，或者直接拷贝 hadoop 目录，使 4 台主机的 xml 文件相同。

```
scp r hadoop hadoop @slave1: /usr/soft/hadoop-2.7.1/
etc/
scp r hadoop hadoop @slave1: /usr/soft/hadoop-2.7.1/
etc/
scp r hadoop hadoop @slave1: /usr/soft/hadoop-2.7.1/
etc/
```

另外，需在 master 和 slave3 节点上配置 slaves 文件，用于指定集群中的 datanode 节点是哪几个。slaves 文件内容如图 6 所示。



```
hadoop@master: /usr/soft/hadoop-2.7.1/etc/hadoop
slave1
slave2
```

图 6 slaves 文件内容

至此，已完成 hadoop 集群的所有必需的配置工作。格式化 hdfs 文件系统，启动 hadoop 集群

格式化 hdfs 文件系统：hadoop namenode format

提示 Storage directory /home/hadoop/hadoop_tmp /
dfs/name has been successfully formatted.

表示 hdfs 格式化成功。

启动 hadoop 集群：start-all.sh

查看各节点的 hadoop 进程信息，使用命令：jps

master 节点进程信息 如图 7 所示。

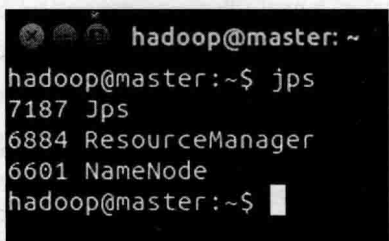


图 7 master 节点进程信息

slave1 节点进程信息如图 8 所示。

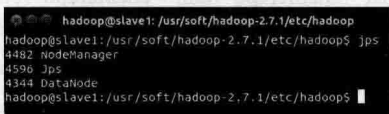


图 8 slave1 节点进程信息

slave2 节点进程信息如图 9 所示。



图 9 slave1 节点进程信息

slave3 节点进程信息如图 10 所示。

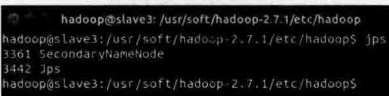


图 10 slave3 节点进程信息

如果以上显示都正常,则表示 hadoop 集群启动成功。

测试 java 程序以验证 hadoop 是否能进行数据分析

本实验将测试 jdk 自带的 wordcount 程序。

先在 master 节点本地创建测试用例：vim test.txt

文本内容：

hello world

hello China

hello Beijing

在 hdfs 文件系统下新建 input 目录：hadoop fs -mkdir /input

查看新建目录是否成功：hadoop fs -ls /

显示有 input 目录了

将 test.txt 从本机上传到 hdfs 文件系统：hadoop fs -put test.txt /input

启动 java 的 wordcount 程序

hadoop jar /usr/soft/hadoop-2.7.1/share/hadoop/mapreduce/hadoop-mapreduce-examples-2.7.1.jar wordcount /input/test.txt /output/

上述语句是一条完整的命令。

启动了 mapreduce，统计文本中单词出现的次数，将结果输出至 output 目录。

查看结果：用浏览器打开 http://master:50070，有了 output 目录，内有 2 个文件 _SUCCESS 和 part-r-00000。

查看 wordcount 统计结果：hadoop fs cat/output/part-r-00000，如果显示结果如图 11 所示，则表示 mapreduce 运算正常。



图 11 查看 wordcount 统计结果

经验总结

Hadoop 集群的 resource manager、namenode、secondary namenode、datanode、nodemanager 等角色搭配比较灵活，也是经常困扰初学者的地方。

几种角色要依赖 4 个 xml 文件和 slaves 来配置，弄清楚这个问题将对进一步学习 Hadoop 至关重要。

利用 ownCloud 建立云盘

吉林 张建鹏

单位员工私人文件存储比较分散，家庭电脑、移动终端、单位电脑都有文件存储，对个人使用文件造成很大的混乱；单位员工之间文件的传递、共享需要解决，一味的依赖移动存储设备大大降低了工作效率，FTP 在众多员工的使用中有很大的局限性。建立云盘这些问题迎刃而解。

为何选择 ownCloud 建立云盘

ownCloud 是自托管文件同步和共享服务软件。它提供了通过 Web 界面、同步客户端或 WebDAV 访问你的数据，同时轻松实现跨平台查看、跨设备同步和共享，这一切都会在你的控制之下的。ownCloud 采用的是开放式架构，它提供了简单而强大的可扩展的 API 的应用程序和插件，适用于任何存储。

ownCloud 的安装过程

我们利用 Centos7+Apache + MariaDB+php 平台来搭建 ownCloud 云盘。

1. 安装 CentOS 7 最小安装，保证能够接入互联网。以下是在 root 用户下完成各种命令及配置。

2. 在 centos7 安装 apache 2.4.6、MariaDB 5.5.44 (MySQL)、php7.0.0。

(1) 安装 apache。

```
yum install httpd
```

(2) 安装 mariadb。

```
yum install mariadb*
```

设置数据库 root 用户密码，后面要用到。

```
mysql -u root
```

```
MariaDB > SET PASSWORD FOR 'root'@'localhost' =PASSWORD('password');
```

(3) 安装 PHP。

a、配置 yum 源

事先确认 yum 源的链接是不是有效的。

```
rpm -Uvh http://ftp.iij.ad.jp/pub/linux/fedora/epel/7/x86_64/e/epel-release-7-5.noarch.rpm
```

```
rpm -Uvh http://rpms.famillecollet.com/enterprise/remi-release-7.rpm
```

b、确认安装的 php 版本

```
yum list --enablerepo=remi --enablerepo=remi-php56 | grep php
```

c、安装 php7

```
yum install --enablerepo=remi --enablerepo=remi-php70 php php-opcache php-pecl-apcu php-devel php-mbstring php-mcrypt php-mysqlnd php-phpunit-PHPUnit php-pecl-xdebug php-pecl-zip php-pdo php-pear php-fpm php-cli php-xml php-bcmath php-process php-gd php-common
```

3. 设置防火墙，启动 apache 和 mysql

```
systemctl start httpd.service
```

```
systemctl enable httpd.service
```

```
systemctl start mariadb.service
```

```
systemctl enable mariadb.service
```

防火墙设置：开启 80 和 443 端口

```
firewall-cmd --permanent --zone=public --add-service=http
```

```
firewall-cmd --permanent --zone=public --add-service=https
```

```
firewall-cmd --reload
```

4. 下载安装 ownCloud

我们采用的是 ownCloud 8.2.1，从官方网站下载 ownCloud8.2.1。运行以下命令：

```
wget https://download.owncloud.org/community/owncloud-8.2.1.tar.bz2
```

解压文件到指定目录：

```
tar -jxvf owncloud-8.2.1.tar.bz2 -C /var/www/
```

如果没有安装 bzip2 一定要安装，否则解压会出现问题。

```
5. 设置 ownCloud 文件及文件夹权限
mkdir /var/www/own cloud/data
find /var/www/own cloud/ -type f -print0 | xargs -0
chmod 0640
find /var/www/own cloud/ -type d -print0 | xargs -0
chmod 0750
chown -R root:apache /var/www/owncloud/
chown -R apache: apache /var/www/owncloud/apps/
chown -R apache: apache /var/www/owncloud/config/
chown -R apache: apache /var/www/owncloud/data/
chown -R apache: apache /var/www/owncloud/themes/
chown root:apache /var/www/owncloud/.htaccess
chmod 0644 /var/www/owncloud/.htaccess
6. 安装 ownCloud 及创建数据库，并进行设置。
$ cd /var/www/owncloud/
$ sudo -u apache php occ maintenance:install --database
"mysql" --database-name "owncloud" --database-user "root"
--database-pass "password" --admin-user "admin" --admin-
pass "password"
```

这里面设置的 database-name 是创建的数据库名，database-user、database-pass 是数据库管理员用户及密码，admin-user、admin-pass 是 ownCloud 管理员用户及密码。显示如下信息标识安装成功：

```
ownCloud is not installed - only a limited number of
commands are available
```

```
ownCloud was successfully installed
设置安装 ownCloud 之后出现的文件权限。
chown root:apache /var/www/owncloud/data/.htaccess
chmod 0644 /var/www/owncloud/data/.htaccess
```

```
7. 修改配置文件 config.php 部分内容如下：
'trusted_domains'=>
array(
0 => 'localhost',
1 => 'server1.example.com',
2 => '192.168.1.50',
),
```

```
8. 修改 apache 配置文件 /etc/httpd/conf/httpd.conf,
设置参数如下：
```

```
DocumentRoot "/var/www/owncloud/"
```

```
<Directory "/var/www/owncloud/">
AllowOverride All
Options Indexes FollowSymLinks
Order allow, deny
allow from all
</Directory>
# 禁止访问 data 文件夹
<Directory "/var/www/owncloud/data/">
Order allow, deny
Deny from all
</Directory>
```

```
9. 设置上传文件大小限制，修改 php.ini 配置文件，
/etc/php.ini
```

```
post_max_size = 800M
upload_max_filesize = 200M
```

```
10. 设置 SELinux 允许 ownCloud 写数据：
```

```
setsebool -P httpd_enable_homedirs=1
setsebool -P httpd_unified 1
```

所有都完成后，重新启动系统，我们的 ownCloud 云盘就建立好了。还可以建立 https 证书，增加系统的安全性。

ownCloud 的使用

（一）管理员用户使用

1. 管理员可以在浏览器地址栏输入 ownCloud 服务器地址，输入之前我们设置好的管理用户名和密码，进入系统 Web 界面。

管理员可以创建用户、组，分配组用户，可以设置组管理员（组管理员有权限创建、管理自己组内的用户），配额每个用户可以使用的空间大小，如图 1 所示。



图 1 ownCloud 管理界面

2. 在管理界面，管理员能够看到安全警告信息、共享设置、版本信息、日志等信息，如图 2 所示。

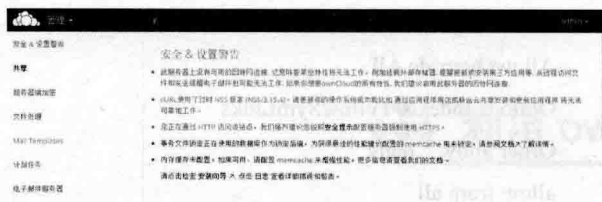


图 2 各种信息

(二) 普通用户使用

普通用户可以有两种方式管理自己的文件：Web 界面和客户端。

1. Web 界面管理方式：

用户在浏览器地址栏输入 ownCloud 服务器地址，输入用户名和密码，进入系统。

在系统的左上角 ownCloud 图标位置显示的“文件”，这是进入系统后显示的主要界面，在这里能够清晰的看到账户管理的文件夹和文件，系统默认建立了 Documents 和 Photos 两个文件夹，在此处可以建立文件夹、上传文件、下载文件、管理文件、分享文件。对于文件分享，可以分享给某一个用户或者一个组（即组内的所有成员），分享文件只能在浏览器方式下进行，如图 3 所示。

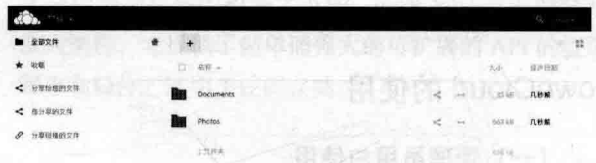


图 3 浏览器管理界面

在系统的左上角 ownCloud 图标位置显示的“文件”处，单击显示下拉菜单，分别显示“文件”、“动态”、“图片”三个选项。“文件”上面已经叙述了。“动态”内显示的相当于个人文件管理日志。“图片”显示的是个人管理的所有图片。

在系统的右上角显示用户名称位置处，单击显示下拉菜单，分别为“个人”、“帮助”、“注销”，如图 4 所示。

“个人”显示个人设置，显示个人的空间使用状态，所属组，可以修改密码，上传个人图片，设置使用的语言，

显示 ownCloud 版本信息等。



图 4 右键菜单

“帮助”，网页的帮助信息，但都是英文的。

“注销”，注销个人登录信息。

2. 客户端管理方式：

可以在计算机终端安装 ownCloud 客户端，这是 ownCloud 系统非常方便的地方，客户端以用户指定的文件夹为管理对象，直接管理此文件夹即可，可以实现登录后与服务器中个人管理的文件及文件夹（包括他人分享给用户的文件）实时同步。但是在这里不能进行个人信息修改，不能进行文件分享。客户端的优势是在个人终端设置完后，可以自动启动，自动登录服务器，非常方便。

这里需要说明一下，分享文件不会重复占用服务器空间，但会同步到客户端。除了计算机客户端，还有手机客户端，这里就不做介绍了。

以上是在 OwnCloud 在免费情况下的应用，还有一些功能如 WebDAV 模式、通讯录、日程等功能只能在收费情况下使用，虽然如此，在免费使用的情况下，已经足够中小型企业的使用了，在 Web 模式和客户端模式配合下，管理文件、传输文件非常方便，这既降低了建立云存储服务费用，同时有效的利用了企业的存储空间和网络，方便员工、部门的文件使用和传递。

❖ Hyper-v Replica 功能详解

▼ 武汉 米泉 严迪 陈浩 闵克锋

企业中有多台 Hyper-v 主机每台 Hyper-v 主机上跑着多个虚拟机，那么如果有一台 Hyper-v 主机出现物理故障宕机后将导致所有虚拟机停止对外提供服务，或者有一台虚拟突然出现宕机，怎么快速恢复正常对外提供服务，怎么解决这个问题呢？可以使用 Windows Server 2012 或者 2012R2 的 Hyper-v 的新功能 Hyper-v 复制来实现虚拟机的副本，这样当一台 Hyper-v 主机或者虚拟机出现故障后，另外一台 Hyper-v 主机上因为有这些重要虚拟机的副本，那么我们启用副本就可以来实现对外的继续提供服务。这里给出了如何使用 Hyper-v 复制的这个功能实现灾备。

测试环境

- 需要两台使用 Hyper-V 角色运行 Windows Server 2012 或 Windows Server 2012 R2 的服务器用于 Hyper-v 的复制（这里主服务器命名 hyper-v，副本服务器命名 hvback）要加入域中。
- 服务器的地理位置，服务器可以在物理上位于同一个位置，也可以位于完全不同的地理位置，主服务器和副本服务器会在同一个防火墙后面应该将防火墙配置为允许复制数据通过。
- 主服务器和副本服务器在物理上共置而且位于同一防火墙后面，则可以使用内置 Kerberos 身份验证。测试拓扑如图 1 所示。

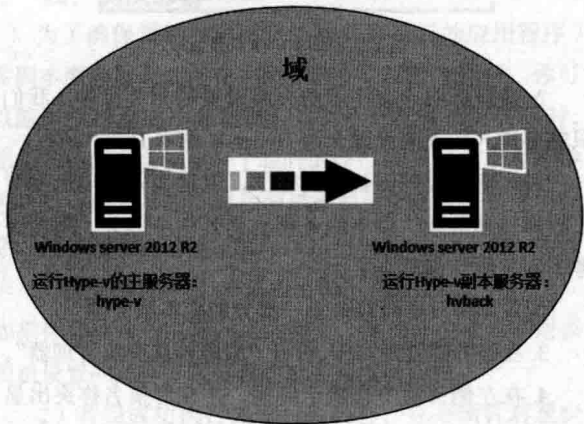


图 1 测试拓扑图

测试步骤

- 一、配置副本服务器
- 二、启用复制
- 三、配置主服务器
- 四、测试部署
- 五、故障转移

下面我们开始逐步讲解步骤：

一、配置副本服务器

1. 在 Hyper-V 管理器中，单击“操作”窗格中的“Hyper-V 设置”，在“Hyper-V 设置”对话框中，单击“复制配置”。在“详细信息”窗格中，选择“将计算机启用为副本服务器”。并选择“使用 Kerberos (HTTP)”端口保持 80 默认，在“授权和存储”选项下，选择“允许从任何经过身份验证的服务器重进行服务”，并指定副本的默认存储位置，可参考图 2 的设置。



图2 指定副本的默认位置

2. 设置后向导会提示防火墙设置的相关警告, 我们只需要进入防火墙设置允许 Hyper-V 副本 HTTP 通过。

到此副本服务器就配置好了, 但是如果公司也配置了故障转移群集, 副本服务器也是其中一部分, 就需要考虑到故障转移群集了。

配置作为故障转移群集一部分的副本服务器

3. 在服务器管理器中, 打开“故障转移群集管理器”。

4. 在左侧窗格中连接至群集, 并在群集名称突出显示之后, 在“详细信息”窗格的“导航”类别中单击“角色”。

5. 右键单击该角色, 然后选择“复制设置”。

6. 在“详细信息”窗格中, 选择“将此群集启用为副本服务器”。

7. 在“身份验证和端口”部分中, 选择你在步骤一: 准备部署 Hyper-V 副本中确定的身份验证方法。对于任一身份验证方法, 指定要使用的端口 (针对通过 HTTP 的 Kerberos, 默认端口为 80; 针对通过 HTTPS 的基于证书的身份验证, 默认端口为 443)。

8. 如果你使用的是基于证书的身份验证, 请单击“选择证书”并提供请求证书信息。

9. 在“授权和存储”部分中, 使用单选按钮指定是允许任何经过身份验证的 (主) 服务器将复制数据发送到此副本服务器, 还是限制从特定主服务器接受数据。你可以使用通配符来限制从特定域接受服务器, 而无需单独指定全部服务器 (例如 *.contoso.com)。如果指定单个主服务器, 则可以为每个服务器的副本数据指定单独存储位置, 也可以使用“信任组”标记对其进行分组。

启用复制

1. 在主服务器 Hyper-V 管理器的“详细信息”窗格中, 通过单击选中虚拟机, 右键单击选定的虚拟机, 然后指向“启用复制”。这将打开“启用复制”向导。在“指定副本服务器”页面的“副本服务器”框中, 输入你在

前面中配置的副本服务器的 NetBIOS 或完全限定的国际域名 (FQIDN), 然后选择启动复制, 如图 3 所示。

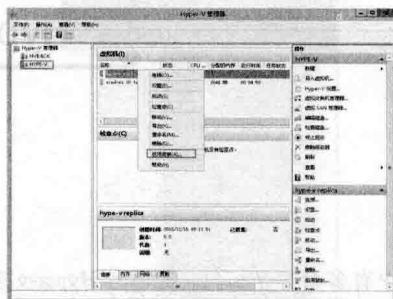


图3 启动复制

2. 指定的副本服务器, 填写服务器名称, 点击“下一步”。

3. 因为之前选择的是仅允许使用 Kerberos 身份验证 (HTTP), 如果网络带宽比较紧张, 建议勾选“压缩通过网络传输的数据”, 继续“下一步”。

4. 选择复制 VHD, 选择要复制的 VHD, 也可以单独将虚机的 VHD 文件拷贝到副本服务器上, 这个根据实际情况而定, 对于附加的 VHD 磁盘或者, 备份用的 VHD 可以不用勾选就不会复制到副本服务器上。

5. 根据需要配置复制频率, 这里我选择的是默认为每 5 分钟将更改发送到副本服务器。

6. 可以根据自己的实际情况去进行选择, 在容灾级别不高, 可以“仅保留最新恢复点”。

7. “选择初始复制方法”下, 可以结合场景并根据实际情况进行选择。如果当前场景是局域网环境, 并且此时网络带宽并不拥挤, 那么可使用默认的“通过网络发送初始副本”作为初始复制方法, 并“立即启动复制”。或者设置启动复制时间, 包括初始复制方法, 就是前面说的 VHD 文件, 也可以根据实际情况在这里通过网络复制, 或者选择介质复制的方式, 在这里我选择的是网络发送并且立即发送, 发送的时间也是蛮快的, 如图 4 所示。



图4 选择通过网络复制

8. 点击完成向导, 就可以看到在发送数据了。

9. 主服务器是正在发送初始副本，副本服务器显示正在接收，如图 5 和图 6 所示。

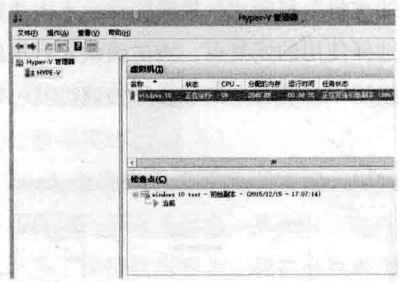


图 5 正在发送数据

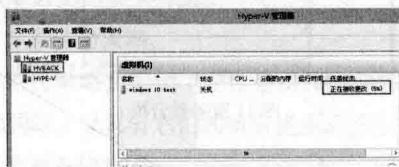


图 6 正在接收数据

10. 发送接收完成之后，可以看到副本服务器上了多了虚机，是关机的，两台不能同时开启，因为信息都是一样的，包括角色，IP 地址等，同时也可以看到主服务器和副本服务器的信息，以及上传同步的时间等，如图 7 所示。

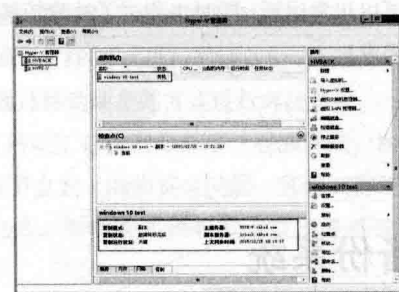


图 7 主副服务器的信息

11. 当然了，根据实际情况如果有需求也是可以副本服务器中的反向复制也是可以将副本服务器变成主服务器。

三、配置主服务器

Hyper-V 副本通常将在主虚拟机上发生的更改发送到副本虚拟机，但在故障转移后，它可反向发送数据。通过执行此操作，当你将操作从当前的主服务器故障转移到副本服务器时，一旦主服务器重新联机可用，即可将复制方向从副本服务器更改回主服务器。通过此方式，可以为目前用于处理虚拟机负载的副本服务器提供复制保护。若要执行此操作，只需使用用于副本服务器的 Hyper-v 上的相同设置即可，如图 8 所示。



图 8 副本服务器的设置

四、测试部署

为了确保复制的虚拟机（和其中运行的应用程序）在副本服务器上如同在主服务器上一样正常运行，你可以随时执行测试故障转移。当你执行测试故障转移时，副本服务器上会创建一个临时的虚拟机。你可以在不中断进行中的复制的同时在测试虚拟机上测试任何应用程序。当你结束测试时，临时虚拟机将会删除。请注意：

1) 在故障转移后，测试虚拟机不会连接到任何网络。如果你必须执行需要网络的测试，则用修改任何普通虚拟机设置的同样方式修改测试虚拟机的设置。

2) 若要成功执行测试故障转移，你必须针对至少一个虚拟机启用了复制，并通过任何可用方法完成初始复制。若要使用最新恢复点以外的恢复点验证故障转移，复制必须运行足够长的时间，以便创建至少一个额外的恢复点。

1. 访问副本服务器，然后在 Hyper-V 管理器中，右键单击要为其测试故障转移的虚拟机，指向“复制…”，然后指向“测试故障转移”。

2. 选择要使用的恢复点。这将创建和启动名称为“<virtual machine name>-Test”形式的虚拟机（例如，“windows 10 test-Test”），如图 9 所示。

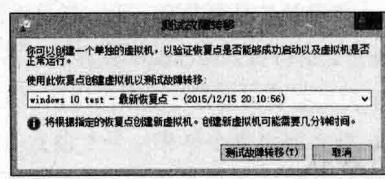


图 9 选择要使用的恢复点

3. 然后可以在测试虚拟机上进行测试。可以验证虚拟机的启动、暂停和停止，以及虚拟机中的任何应用程序是否正常运行。在结束了测试之后，通过选择“复制”选项下的“停止测试故障转移”放弃测试虚拟机。如果要删除同步复制的状态，在复制下面点击删除复制即可，如图 10 所示。

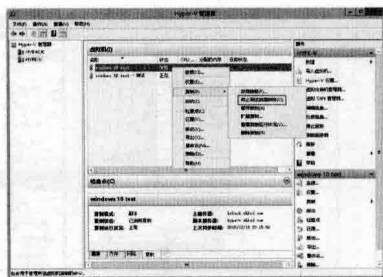


图 10 选择要使用的恢复点

五、测试故障转移

分为三种：

1. 计划内故障转移，顾名思义也就是按照预先确定的计划来进行故障转移。该方式需要满足两个前提条件：在初始故障转移前，虚拟机必须关闭；主服务器也必须启用复制功能，并允许接收来自副本服务器的复制，注意要先关机才能执行故障转移。

这样的话，就成功的进行了转移，可以看到在副本服务器上，转移的虚拟机正常运行，没有文件丢失。

2. 测试故障转移，在副本服务器上进行操作，允许在不中断当前持续的复制配置下，生成并启动一个新的用于测试用途的虚拟机

3. 计划外故障转移，主服务器意外宕机时，我们便可以在副本服务器上执行“故障转移”，将该虚拟机启动上线。

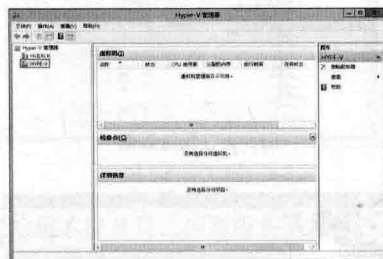


图 11 服务器宕机

结语

通过 Windows Server 2012/2012 R2 下的 Hyper-v 复制的功能我们可以实现 Hyper-v 主服务器的整体灾备，同时也是定期的复制，如果发生问题，可快速在副本服务器上启动服务，复制的虚拟机角色和 IP 地址都不会发生变化。可以正常运行，同时也测试了故障转移的情况，可以实现需求！

搭建网络数据备份系统

广东 王晓鹏

数据备份现状

在信息系统安全等级保护工作中，围绕计算机系统所采取的许多安全保护措施最终都是为了保证系统中数据在应用、存储、传输和处理过程中的安全性，以实现数据的机密性、完整性、可控性和不可否认性，并可以进行数据备份和恢复。本文主要关注其中的数据备份工作。

(1) 数据安全风险

数据安全威胁主要来自以下几种形式：

1) 数据存储设备故障。这是最普通的情况，随着数据存储设备性能的提高与改进，这种故障会进一步减少。

2) 数据存储介质损坏。这里包括机械性毁损和电磁性毁损，包括人为因素造成的损坏、意外事件造成的损坏和介质寿命因素造成的损坏等。通过使用冗余设备，这种故障能得到有效抑制。

3) 各种天灾造成的损坏。包括地震、海啸和山崩等地质灾害，以及风灾、水灾、雪灾、火灾、低温和高

温等灾害造成的数据系统损坏。

4) 衍生灾害。天灾人祸都可能引发生性灾害,可能造成电力系统、天、地通信系统等损坏,导致数据系统损坏。

5) 人为无意因素造成对数据误操作引发的数据损失,甚至是数据灾难。

6) 人为有意因素造成的数据损坏。例如黑客、病毒和恶意程序攻击等有意因素,都会对数据造成破坏。

为此,为了保障数据安全,我们必须根据数据的重要性和本单位的实际,采取相应的数据备份策略和备份技术来保障数据的安全可用。

(2) 数据备份策略

差异备份策略在避免了完全备份和增量备份两种策略缺陷的同时,又具有它们的所有优点。

(3) 数据备份技术

数据备份技术主要有双机热备、数据冷备份、数据异地备份等等。

我们单位目前主要采取的数据备份策略是异地磁盘每周全份、每天增备,而数据备份方式主要有:

- 1) 采购有授权备份节点数限制的备份软件对重要的几台服务器的数据进行备份;
- 2) 通过创建快照或者克隆对虚拟机进行备份;
- 3) 通过 FTP 方式进行网络备份;
- 4) 通过移动硬盘的方式进行离线备份。

现有的手工备份工作繁琐、查漏麻烦,购买商业软件的授权节点数又面临资金问题。那现在需要备份的数据越来越多,继续购买授权节点数还是继续手工备份呢?

我们在此过程中,一直在考虑其他性价比高的解决方案。比如是否可以通过开源软件进行备份,并把它集成进我们最近构建的开源网络运维统一平台,实现与其他网络管理工作在同一个平台里统一管理,而不需要多个平台去管理或是手工去操作导致无法统一管理。

Rsync 远程同步工具简介

Rsync 是类 UNIX 系统下的数据镜像备份工具——Remote sync (远程同步),它是一个远程数据同步工具,可通过 LAN 或互联网快速同步多台主机间的文件。

Rsync 本来是用以取代 rcp 的一个工具,它当前由 rsync.samba.org 维护。Rsync 使用所谓的“Rsync 演算法”来使本地和远程两个主机之间的文件达到同步,这个算

法只传送两个文件的不同部分,而不是每次都整份传送,因此速度相当快。

(1) Rsync 特性

1) 镜像:可以镜像保存整个目录树和文件系统,可以很容易做到保持原来文件的权限、时间、软硬链接等等;

2) 快速:第一次同步时 Rsync 会复制全部内容,但在下一次只传输修改过的文件;

3) 省带宽:Rsync 在传输数据的过程中可以实行压缩及解压操作,因此可以使用更少的带宽;

4) 安全:可以使用 scp、ssh 等方式来传输文件,当然也可以通过直接的 socket 连接,支持匿名传输,以方便进行网站镜像;

5) 特权:安装和执行 Rsync 无需特别的权限。

(2) Rsync 同步算法

Rsync 之所以同步文件的速度相当快,是因为“Rsync 同步算法”能在很短的时间内计算出需要备份的数据,关于 Rsync 的同步算法描述如下:

假定在 1 号和 2 号两台计算机之间同步相似的文件 A 与 B,其中 1 号对文件 A 拥有访问权,2 号对文件 B 拥有访问权。并且假定主机 1 号与 2 号之间的网络带宽很小。那么 Rsync 算法将通过下面的五个步骤来完成:

- 1) 2 号将文件 B 分割成一组不重叠的固定大小为 S 字节的数据块,最后一块可能会比 S 小;
- 2) 2 号对每一个分割好的数据块执行两种校验:一种是 32 位的滚动弱校验,另一种是 128 位的 MD4 强校验;
- 3) 2 号将这些校验结果发给 1 号;

4) 1 号通过搜索文件 A 的所有大小为 S 的数据块(偏移量可以任选,不一定非要是 S 的倍数),来寻找与文件 B 的某一块有着相同的弱校验码和强校验码的数据块。这项工作可以借助滚动校验的特性很快完成;

5) 1 号发给 2 号一串指令来生成文件 A 在 2 号上的备份。这里的每一条指令要么是对文件 B 经拥有某一个数据块而不须重传的证明,要么是一个数据块,这个数据块肯定是没有与文件 B 的任何一个数据块匹配上的。

必须同时在备份源服务器 A 和备份目标服务器 B 上都安装 Rsync,其中服务器 A 上是以服务器模式运行 Rsync,而服务器 B 上则以客户端方式运行 Rsync。这样在服务器 A 上运行 Rsync 守护进程,在备份服务器 B 上定时运行客户程序来备份源服务器 A 上需要备份的内

容。

统一网络数据备份系统建设方案

根据学校的数据备份的实际需求和开源工具的比较,我们选择比较成熟的 Rsync 软件在实现数据同步的同时,把同步日志发送到以 Cacti 为基础搭建的统一网管平台的 Syslog 模块里进行统一管理,结合统一网管平台的 Threshold 模块实现异常报警,构建统一网络数据备份系统,具体建设方案如下:为基础,在 Linux 下用 Rsync+Syslog、在用 cwRsync+NTsyslog,

(1) 基本备份功能

基本备份功能通过免费软件 Rsync 实现,linux 和 windows 操作系统都有相应的 Rsync 软件。

1) 安装 Rsync 软件

Centos 下安装 Rsync 的命令为 yum install rsync。

windows 下安装 cwRsync 则是下载经典免费版本 cwRsyncServer-v4.1.0,按默认方式安装即可。

2) 配置服务器端

Centos 下配置 Rsync 的命令为 vim /etc/rsyncd.conf, Windows 下的配置文件路径则为“C:\Program Files(x86)\ICW\rsync.conf”。

以下以 Windows 下的配置文件为例,Centos 下类之:

全局参数开始

use chroot = false # 如果“use chroot”指定为 true,那么 Rsync 在传输文件以前首先 chroot 到 path 参数所指定的目录下。这样做的原因是实现额外的安全防护,但是缺点是需要 root 权限,并且不能备份指向外部的符号连接所指向的目录文件,默认情况下 chroot 的值为 true

strict modes = false # 该选项指定是否监测密码文件的权限,如果该选项值为 true,那么密码文件只能被 rsync 服务器运行身份的用户访问,其他任何用户不能访问该文件,默认值为 true

hosts allow = 192.168.1.100 # 指该选项指定哪些 IP 的客户允许连接该模块。客户模式定义可以是以下形式:单个 IP 地址,例如:192.167.0.1;整个网段,例如:

192.168.0.0/24,也可以是 192.168.0.0/255.255.255.0。

多个 IP 或网段需要用空格隔开,“*”则表示所有,默认是允许所有主机连接。

hosts deny = * # 指定不允许连接 Rsync 服务器的机器,可以使用 hosts allow 的定义方式来进行定义。默认

是没有 hosts deny 定义。

log file = rsyncd.log # 指定 Rsync 的日志文件,而不把日志发送给 syslog

为了集中管理日志,上行需注释掉,以便 log 不存在本地而是发到 syslog

pid file = rsyncd.pid # 指定 Rsync 的 pid 文件

port = 873 # 指定服务运行端口,默认是 873

uid = 0 # 不指定用户 id,不加这一行将无法使用任何账户

gid = 0 # 不指定用户组 id

max connections = 10 # 指定该模块的最大并发连接数量以保护服务器,超过限制的连接请求被告知随后再试。默认值是 0,也就是没有限制。

全局参数结束

以下为模块参数,我们可以通过根据自己的需要,来指定多个模块

Module definitions

Remember cygwin naming conventions: c:\work becomes /cygwin/c/work#

模块 test 参数开始

[test]

path = /cygdrive/c/work # 指定该模块的供备份的目录树路径,该参数是必须指定的

read only = false # 该选项设定是否允许客户上载文件,如果为 true 那么所有的上载请求都会失败,如果为 false 并且服务器目录读写权限允许那么上载是允许的,默认值为 true。

transfer logging = yes # 使 Rsync 服务器使用 ftp 格式的文件来记录下载和上载操作在自己单独的日志中

lock file = rsyncd.lock # 指定支持 max connections 参数的锁文件

#auth users = service-scada # 认证用户名

#secrets file = rsync.password # 认证用户的用户名和密码存储位置

模块 test 参数结束

(2) 定期执行功能

定期执行功能通过操作系统的计划任务实现。

1) Centos 下通过 crontab 命令加入操作系统的计划任务

crontab -e

01 00 * * * rsync -azu --password-file=/etc/rsyncd.password --progress root@192.168.1.1::test /home/

```
backup/192.168.1.1/ > /dev/null 2>&1
```

此计划任务为每天凌晨 1:00 以 root 用户和指定的 /etc/rsyncd.password 文件内保存的密码登录 192.168.1.1, 把 192.168.1.1 的 test 模块里的文件夹同步到本地的 /home/backup/192.168.1.1/ 目录, 同步参数为 azu(其中 -a, --archive 归档模式, 表示以递归方式传输文件, 并保持所有文件属性, 等于 -rlptgoD; -z, --compress 对备份的文件在传输时进行压缩处理; -u, --update 仅仅进行更新, 也就是跳过所有已经存在于 DST, 并且文件时间晚于要备份的文件, 不覆盖更新的文件)

我们亦可以通过写 shell 脚本来实现丰富功能, 比如实现每 7 天全备、每天差备, 调用系统的 mailx 软件在同步异常或恢复时发送邮件通知。

2) windows 下通过系统控制面板里的计划任务来实现

建立 bat 文件内容如下:

```
c:
cd C:\Program Files(x86)\ICW\bin
rsync -azu rsync://192.168.1.1/test /cygdrive/
d/192.168.1.1
```

然后在控制面板的计划任务里面添加相应的任务即可。

Windows 下亦可以通过 bat 脚本调用 vb script 来实现以上 Centos 里用 shell 来实现的丰富功能。

(3) 服务监控功能

服务器在安装好 Rsync 软件后, 可能在后续的系统更新或是安装其他软件中破坏了 Rsync 服务而导致无法同步。那么我们能不能像监控网页、数据库服务一样来对此服务进行实时监控呢?

我们可以选择 Windows 下的 hostmonitor、whats up 等服务监控软件进行监控, 而笔者此处是选择了已经集成在网络运维统一平台里的 Nagios 模块对此服务进行实时监控, 并在服务异常时调用 Threshold 发送邮件报警。

(4) 收集日志功能

我们在前面的 Rsync 的配置文件 rsync.conf 中提到需要注释 log file = rsyncd.log 以便 Rsync 软件把日志作为系统日志 syslog 处理。

在 Unix 类操作系统上, syslog 广泛应用于系统日志。syslog 日志消息既可以记录在本地文件中, 也可以通过网络发送到接收 syslog 的服务器。接收 syslog 的服务器可以对多个设备的 syslog 消息进行统一的存储, 或者解

析其中的内容做相应的处理。常见的应用场景是网络管理工具、安全管理系统、日志审计系统。

修改备份源服务器的 /etc/syslog.conf 文件, 在有关配置行的操作动作部分用一个 “@” 字符 + 日志服务器 IP。如

```
*.* @192.168.1.200
```

在 Windows 操作系统下没有自带 syslog 客户端软件, 但可以通过安装 NTSyslog 软件来实现把系统日志转发到指定的日志服务器。

笔者的日志服务器为用 Cacti 搭建的网络运维统一平台里的服务器, 通过其中的 Syslog 模块来查看相应的服务器、防火墙、交换机、IPS 等日志, 此处特别针对 Rsync 的日志做了二次开发, 以方便在 Syslog 模块下查看。

(5) 实时同步功能

与传统的 cp、tar 备份方式相比, Rsync 具有安全性高、备份迅速、支持增量备份等优点, 通过 Rsync 可以解决对实时性要求不高的数据备份需求, 例如定期的备份文件服务器数据到远端服务器, 对本地磁盘定期做数据镜像等。

随着应用系统规模的不断扩大, 对数据的安全性和可靠性也提出的更好的要求, Rsync 在高端业务系统中也逐渐暴露出了很多不足, 首先, Rsync 同步数据时, 需要扫描所有文件后进行比对, 进行增量传输。如果文件数量达到了百万甚至千万量级, 扫描所有文件将是非常耗时的。而且正在发生变化的往往是其中很少的一部分, 这是非常低效的方式。其次, Rsync 不能实时的去监测、同步数据, 虽然它可以通过 linux 守护进程的方式进行触发同步, 但是两次触发动作一定会有时间差, 这样就导致了服务端和客户端数据可能出现不一致, 无法在应用故障时完全的恢复数据。基于以上原因, Rsync+Inotify 组合出现了!

Inotify 是一种强大的、细粒度的、异步的文件系统事件监控机制, linux 内核从 2.6.13 起, 加入了 Inotify 支持, 通过 Inotify 可以监控文件系统中添加、删除、修改、移动等各种细微事件, 利用这个内核接口, 第三方软件就可以监控文件系统下文件的各种变化情况, 而 Inotify-tools 就是这样的一个第三方软件。

Rsync 可以实现触发式的文件同步, 但是通过 crontab 守护进程方式进行触发, 同步的数据和实际数据会有差异, 而 Inotify 可以监控文件系统的各种变化, 当文件有任何变动时, 就触发 Rsync 同步, 这样刚好解决

了同步数据的实时性问题。

所以,如果业务系统对数据同步的实时性要求很高,要求实现正式服务器一旦出现故障,则备份服务器可以马上上线这样的类似容灾系统的功能的话,我们可以通过先克隆虚拟机到异地,再在正式服务器上安装 Inotify (Windows 下也支持管道符,可以通过 Inotifywait 再结合自己写脚本来实现)。

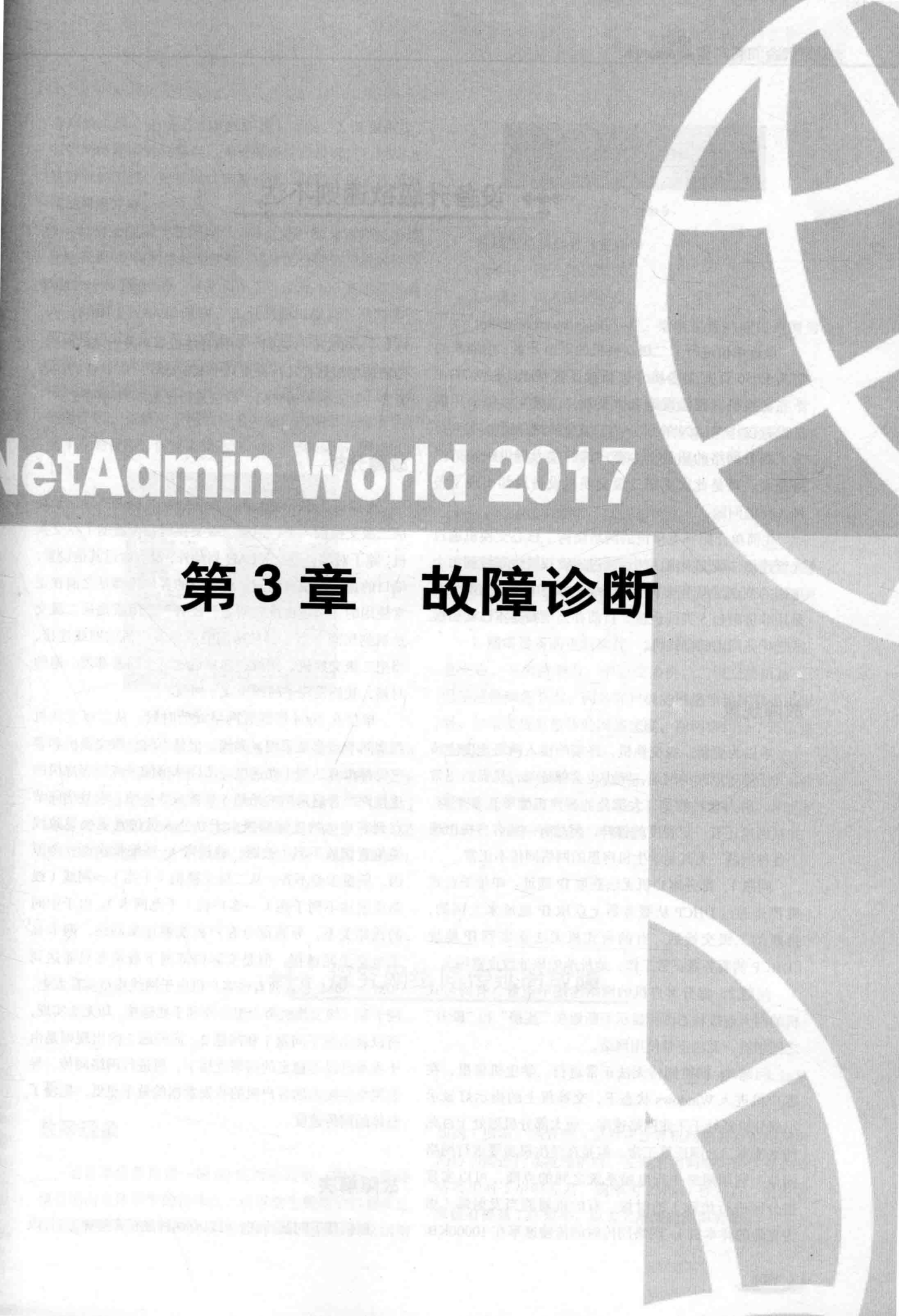
结语

通过采用多个免费工具的整合,实现统一网络数据备份系统,并把日志和服务监控集成进网络运维统一平台进行集中管理。

下一步的工作是把数据备份作业的配置和最近一次运行状态通过图形化来查看管理,以提高工作效率。

NetAdmin World 2017

第3章 故障诊断



设备升级欲速则不达

浙江 戴峰

最近单位进行了二级交换机的更换升级，由原来的华为 E050 百兆交换机，更新成了锐捷 RG-S2952G-E 千兆交换机，其他设施未做更新，二级交换机采用默认设置仅作 VLAN 的划分。二级交换机的更新本来是为了提升网络的质量，为客户机的接入提供稳定的网络速度。可是此次更新二级交换机设备后却出现了各种各样的问题。

先简单介绍一下单位的网络结构：核心交换机通过光纤连接二级交换机，然后通过 6 类双绞线布线到每个房间的节点，但是从节点到终端（办公电脑）大部分都是用非屏蔽超 5 类线连接。目前办公电脑基本已经更换成带千兆网卡的台式机。

故障现象

本以为更新二级交换机，终端的接入网络速度应该会大于等于原来的网速，至少也会保证每台机器的正常上网。出人意料的是，大部分的客户机能够正常上网，并且网速还有一定程度的提升，但是有一些客户机出现了各种问题，尤其是学生机房里的网络同传不正常。

问题 1，部分客户机无法获取 IP 地址。单位的台式机都是通过 DHCP 从服务器上获取 IP 地址来上网的，换新的二级交换后，有的台式机无法获取到 IP 地址（DHCP 的服务器正常工作，地址池的地址数也够用）。

问题 2，部分客户机的网络连接不正常。有的台式机的网卡连接状态图标显示不断地在“连接”和“断开”之间切换，无法正常使用网络。

问题 3，网络同传无法正常进行。学生机房里，在客户机进入 Windows 状态下，交换机上的指示灯显示小部分机器处于千兆网络速率，而大部分机器处于百兆网络速率，上网还算正常。但是在学生机房要进行网络同传（利用网络进行电脑系统之间的克隆，可以实现按分区进行传输）的时候，有的机器能当发射端（做为克隆的样本机），网络同传时的传输速率在 10000KB/

秒 ~ 11000KB/秒之间，而用有些机器当发射端的时候，传输速率却只有几百甚至几十 KB 每秒，几十 G 的内容需要一整天的传输时间，没法进行正常的网络同传。

故障分析

考虑到出现上述问题是在二级交换机更换后，于是从二级交换机入手，但是二级交换机是全新的千兆交换机，除了对端口进行 VLAN 划分外，没有做过其他设置，端口的速度都是自适应。而单位的客户机都是之前在正常使用的，应该也没有问题。还有一个因素是从二级交换机到房间节点，再从房间节点到客户机的网线连接。当把二级交换机、网线、客户机这三个因素都理一遍的时候，我们发现了问题所在：网线。

单位在 2004 年部署网络线的时候，从二级交换机到房间节点都是采用 6 类线，但是那时二级交换机和客户机都没有达到千兆速度，所以从房间节点到客户机的连接网线普遍采用的是超 5 类线或 5 类线，而且房间节点到客户机的连接网线由于办公人员位置更换导致线缆位置摆放不当（被踩、被折弯）、线缆批次不一等原因，质量参差不齐。从二级交换机（千兆）→网线（线路质量达不到千兆）→客户机（千兆网卡），由于中间的线路关系，导致部分客户机能够连接网络，网卡显示也是千兆链接，但是实际内部网下载速度只能达到 30M ~ 50M/秒，而有些客户机由于网线质量实在太差，网卡和二级交换机努力想协商到千兆链接，却无法实现，所以就出现了问题 1 和问题 2。而问题 3 的出现则是由于本身已经不稳定的网络连接下，再进行网络同传，导致网络连接差的客户机的收发数据的效率更低，拖慢了整体的同传速度。

故障解决

搞清楚了问题所在，可以有两种途径来解决它：1. 改

善网线质量，把所有 5 类线换成 6 类线。2. 降低网速，保持网络连接的稳定性。考虑到现阶段没有进行网络改造升级的工程，更换网线比较麻烦，我们采取了降低网速的解决方案。

1. 对于问题 1 和问题 2，由于是少部分客户机出现无法获取 IP 和网络断断续续，将这部分的客户机的网卡配置——高级里的“速度和双工”改成 100 兆全双工即可（如图 1 所示）。这时，二级交换机就会自动与客户机协商成 100 兆全双工链接，保持链接的稳定性。经测试，客户机在内部网络的下载速度能够达到 8M ~ 10M/ 秒，能满足现阶段的网络应用需求。而那些能够链接为千兆的客户机，虽然由于网线质量问题，内网下载速度达不到千兆的目标，但是也能达到 300 ~ 500Mbps 的速度。

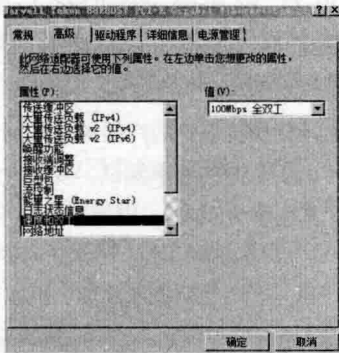


图 1 设置为“100 兆全双工”

2. 对于问题 3，机房里的网络同传不正常的问题。由于修改每台机器的网卡链接速度太麻烦，采用修改交换机的端口链接速度的方法达到降速的目的。可以通过 telnet 或者交换机的配置口连接交换机进行配置，本文采用超级终端连接锐捷交换机配置口的方法（如图 2 所示）。

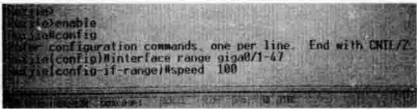


图 2 配置命令

锐捷交换机部分命令解释：

Enable：进入特权模式。

Config：进入配置模式。

Interface range gigabitEthernet 1/47：指定配置的端口范围为 1-47 端口。

Speed 100：配置速率为 100Mbps。

经过交换机降速后，机房的网络同传恢复正常，任意一台机器作为发射端，网络传输速度都能保持在 10000KB/ 秒左右，符合百兆网络的速度。

经验总结

网络的升级、改造是每个单位都会面临的现状，通过本单位的案例，个人觉得有两点值得在我们开展相关工作时作为参考：

1. 网络设备的更新换代一定要统筹考虑，不能只注重中心，不关注细节。中心交换机、二级交换机重要，但是连接到各节点、到各客户机的网络质量同样不可忽略。如果要提升整体的网络速度，在网络的每个环节都要跟上。

2. 网络速度提升，需要每一个环节都达到标准，欲速则不达。如果网络在高速时不稳定，我们不妨对其进行降速，待条件符合时再提速。

探究网络同传延时故障

贵州 朱红军

故障现象

笔者单位新构建一间 60 座网络教室，由于工作环境是面向全体学生的特殊性，所以学生使用的机器要选择具有网络同传和实时还原功能的台式电脑，网络结构

如图 1 所示。当管理人员对该计算机网络教室运用网络同传功能进行系统维护时，发现采用网络同传恢复系统需要用时 5 小时左右，速率为 2Mbps/ 秒左右。使用效果没有提高工作效率，也大大地浪费能源资源。

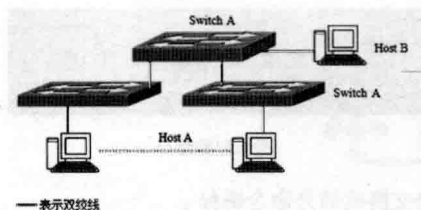


图1 网络结构

说明：Switch A 带管理功能的 S3026G 交换机；Host A 为学生机；Host B 为教师机。

故障排查

通过对网络构建结构分析，问题可能出在交换机上，并通过调整网络结构如图 2 所示进行故障排除、定位。

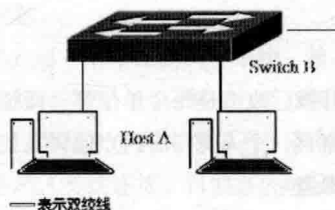


图2 调整网络结构

通过对图 2 结构网络同传测试发现，接入在 Switch B（非管理功能的普通接入层交换机）的学生机进行网络同传时，其速率为 50Mbps/ 秒左右。

综合以上测试分析，可以定位故障原因发生在 Switch A 交换机上。问题可能是因交换机的广播风暴抑制配置上。于是，登录到交换机的配置模式，使用 show storm-control 命令 查看 f0/1-f0/24 端口广播风暴抑制状态，状态为开启状态。

故障处理

影响网络同传速率的原因应是交换机开启端口广播风暴抑制功能所导致的。分别运用下列 interface range fastEthernet 0/1-24、no storm-control broadcast、no storm-control multicast、no storm-control unicast 命令关闭交换机端口的广播风暴抑制。

通过配置好交换机端口的广播风暴抑制功能后，笔者对网络同传做了全面的速率测试，发现有效提高了网络同传速度，其速率为 50Mbps/ 秒左右。

交换机级联端口被绑之后

济南 王德安 韩冰

故障现象

某单位新增一台计算机，用户根据周边上网终端 IP 地址分配规律，配上未使用的 IP 地址，发现不能上网，遂上报单位网管请求解决。新上任网管根据网络安全管理要求，远程操作楼层交换机，按照“交换机端口 + 终端 MAC + 终端 IP”方式进行绑定，操作完成后用户还是不能上网，而后又有其他楼层用户反映不能上网。单位网管也无法远程联接刚刚操作的楼层交换机了，单位网管请求技术支持。

故障排查

经现场了解得知，出现故障大楼的简单网络拓扑结构如图 1 所示，整个大楼网络终端设备都属于同一个 VLAN，各楼层所属交换机采取级联方式，汇聚到大楼交换机后再与单位三层路由交换机相连。网络终端乙为新增上网终端，接入楼层交换机 B2。楼层 N2 的其他终端能正常上网，楼层 N1 的所有终端不能上网。网管在机房不能远程联接管理楼层 N1 的所有交换机。综合判断为楼层交换机配置出了问题。

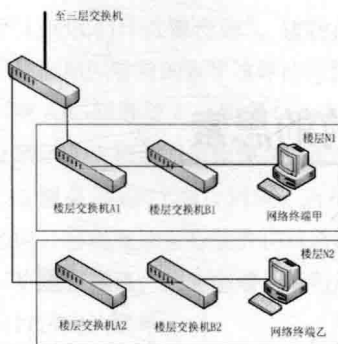


图 1 网络拓扑结构图

查询 H3C 交换机端口绑定命令为：

```
interface eth 1/0/xx
am user-bind mac xxxx- xxxx - xxxx ip xxx.xxx.xxx.
xxx
```

进一步查阅资料得知，H3C 交换机的级联端口不能被绑定终端，否则该交换机的接入用户终端不能正常上网。

再回顾一下单位网管的绑定操作流程：（1）用 telnet 命令远程登录楼层交换机。（2）用 dis mac-address 命令查看交换机端口与终端 MAC 地址对应情况（如图 2 所示），找到新增用户对应的端口号。（3）执行绑定命令。

接口名称	VLAN ID	MAC 地址	端口名称
Ethernet1/0/1	1	0000-0000-0000	001000
Ethernet1/0/2	1	0000-0000-0000	001001
Ethernet1/0/3	1	0000-0000-0000	001002
Ethernet1/0/4	1	0000-0000-0000	001003
Ethernet1/0/5	1	0000-0000-0000	001004
Ethernet1/0/6	1	0000-0000-0000	001005
Ethernet1/0/7	1	0000-0000-0000	001006
Ethernet1/0/8	1	0000-0000-0000	001007
Ethernet1/0/9	1	0000-0000-0000	001008
Ethernet1/0/10	1	0000-0000-0000	001009
Ethernet1/0/11	1	0000-0000-0000	001010
Ethernet1/0/12	1	0000-0000-0000	001011
Ethernet1/0/13	1	0000-0000-0000	001012
Ethernet1/0/14	1	0000-0000-0000	001013
Ethernet1/0/15	1	0000-0000-0000	001014
Ethernet1/0/16	1	0000-0000-0000	001015
Ethernet1/0/17	1	0000-0000-0000	001016
Ethernet1/0/18	1	0000-0000-0000	001017
Ethernet1/0/19	1	0000-0000-0000	001018
Ethernet1/0/20	1	0000-0000-0000	001019
Ethernet1/0/21	1	0000-0000-0000	001020
Ethernet1/0/22	1	0000-0000-0000	001021
Ethernet1/0/23	1	0000-0000-0000	001022
Ethernet1/0/24	1	0000-0000-0000	001023
Ethernet1/0/25	1	0000-0000-0000	001024
Ethernet1/0/26	1	0000-0000-0000	001025
Ethernet1/0/27	1	0000-0000-0000	001026
Ethernet1/0/28	1	0000-0000-0000	001027
Ethernet1/0/29	1	0000-0000-0000	001028
Ethernet1/0/30	1	0000-0000-0000	001029
Ethernet1/0/31	1	0000-0000-0000	001030

图 2 查看交换机端口与终端 MAC 地址对应情况

分析操作流程，断定网管在楼层交换机 A1 上对网络终端乙进行了绑定，导致楼层 N1 所有用户终端不能上网。

故障解决

需要解决以下两个问题：

1. 去除楼层交换机 A1 对上级联端口绑定设置，解决楼层 N1 所属终端不能上网问题。

找 1 台接入楼层交换机 A1 的终端，用 telnet 命令远程登录楼层交换机 A1，执行如下命令：

```
dis am user-bind
interface eth 1/0/X
undo am user-bind mac xxxx - xxxx - xxxx ip xxx. xxx.
xxx. xxx
```

注：第 1 行是显示交换机端口绑定情况，找到向上级联端口的绑定信息。第 2 行是进入 1/0/x 端口，该端口是楼层交换机 A1 向上级联端口。第 3 行是去除绑定设置，即将绑定的 MAC 地址和 IP 地址取消。

当然，以上步骤也可使用便携式笔记本电脑，用专用连接线直接对接楼层交换机 A1 的管理端口，通过超级终端操作实现。

2. 登录楼层交换机 B2，对新增网络终端乙进行绑定。首先需要找到对应端口，然后才能执行绑定。

注意：所有对交换机的操作，要执行 save 命令，否则断电重启后会恢复原样。

经验总结

至此，楼层 N1 网络恢复正常，网络终端乙也能上网了。细想起来，这是一起由于新上任网管没有找准网络终端乙对应的楼层交换机而造成的误配。为什么会这样呢？新增加某终端，同一 VLAN 内所有二层交换机都能收到这台新增终端的 MAC 地址，只是直连交换机登记在直连端口上，其他交换机登记在级联端口上，一般情况下在直连端口做绑定，但新上任网管没有区分这些细微之处，导致网络故障。所以说，网络管理无小事，对症下药很关键。

使用重启大招之前的思索

广东 赖文书

故障现象

周六休息时,突然接到实验室同事报障电话,说就在刚才断电 10 分钟来电后,OpenLAB 系统无法连接。机房服务器有 UPS 供电,怎么会出现这样的情况呢?赶到现场查看,机房里整套系统 7 台服务器从电源、硬盘和网络指示灯看均运行正常,登录一台服务器表面上看也没有问题,只是用户在办公室通过远程桌面打开 OpenLAB 软件时,一直显示连接中(如图 1 所示)。在机房 AIC 服务器上打开 OpenLAB 软件,仍然是同样的情况。也就是说,所有用户都无法正常启动该软件。



图 1 OpenLAB 软件启动一直连接中

系统介绍

由于周末只有个别用户加班,所以影响还算小,可以有时间来仔细检测问题原因。只是从同事那儿接手该系统两年来,没有遇到过类似情况,平日也就是每两周把所有服务器重启一次,协助厂家工程师安装过增加的系统,因一台反应慢更换过服务器,还有就是每月一次的通过 SSR 系统备份和每周用 BE 备份试验数据。

OpenLAB CDS 网络化色谱工作站系统是安捷伦公司基于微软 .NET 技术,拥有三层体系结构,由 OpenLAB OLSS 服务器、Agilent AIC 和瘦客户端三层组成。OLSS 服务器负责提供系统的安全管理、许可审核、审计追踪、仪器状态管理以及数据存储等功能。Agilent Instrument Controller (以下简称 AIC) 作为系统的中间层,负责提供数据的采集、仪器的反控、数据的缓存以及上传等工作。客户端使用远程桌面服务虚拟客户端模式,利用微软的 RDS 虚拟技术,可以实现客户端的零

安装。全套系统操作系统均是 Windows Server 2008 R2 英文版,曾听同事讲过几次系统的大概结构:用户通过 TS 终端服务器的远程桌面方式去操作控制 AIC 服务器所连接的仪器,用户登录远程桌面是通过端服务器的本地验证,OpenLAB 软件登录验证是通过 OLSS 服务器进行的,最后将仪器生成数据存入 ECM 服务器。

排错与测试

首先通过 Ping 命令确认了服务器间通讯正常;其次查看服务器日志,在下午 2:34TS 服务器有错误日志“The Terminal Server security layer detected an error in the protocol stream and has disconnected the client. Client IP: 192.168.219.55.”,也就是当天来电后加班同事的连接,其他时段还有大量类似报错;在下午 2:24AIC 服务器有两条错误日志“The Terminal Server security layer detected an error in the protocol stream and has disconnected the client. Client IP: 192.168.17.10.”也就是在停电时 AIC 终端服务安全层检测到 TS 服务器在协议流中有错误而断开了连接,同时仪器驱动也报了两条错误日志“Disconnecting because a System.Net.WebException was caught when sending a command; The request was aborted: The operation has timed out.”,但是这条日志该服务器在其他时间段也大量出现过,用户那边未曾报告出现什么问题。

由于周末厂商直接售后服务的工程不方便联系,于是拨打了安捷伦售后服务电话,服务人员得知是 OpenLAB ChemStation 的网络版时,说这种情况涉及到网络方面的原因,没有网络工程师值班而无法解答,建议重启服务器系统试试。咨询结果和预期的一样,使用服务器重启大招。旁边实验室的同事说这样的问题是第二次出现了,上次也是停电后发生的,那次他以为是我们 IT 人员在处理服务器上午有问题也未反馈,下午

就正常了（而我们什么都没做）。这就很奇怪了，很想探研一下什么原因导致的发生这样的问题。

再回到 AIC 服务器上，发现 OpenLAB 程序有报错了如图 2 所示，大概意思是程序在已配置的 3 分钟内未获得 OLSS 服务器 6577 端口回应，运行中分配的时间已部分超时，可能是该运行服务仍然在进行中或者是未能发出一个应答信息，请考虑增加运行超时设置并确保客户端可以访问该服务。

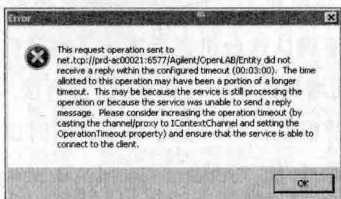


图 2 软件启动报错提示

有了错误提示，就多一些处理问题的线索，通过 telnet 服务器 OLSS 端口 6577 是通的，为什么端口是正常能连接而程序却无法连接呢？登录 OLSS 服务器 netstat 查看端口连接情况，显示很慢很多，有大量 TS 服务器到 OLSS 服务器 6577 端口的连接（如图 3 所示）。难道是端口异常繁忙导致无法给程序响应？可是现在周末没几个用户，而且平日也从来没有出现这种现象啊。

[illegible]

图 3 OLSS 服务器 netstat 显示端口连接 a

把 TS 服务器重启一下再看是什么现象，因为重启 TS 对数据没有任何影响，比直接重启 OLSS 服务器影响小。后又想，直接把 TS 服务器的网线拔掉也能验证刚才的想法。

拔掉服务器实验网段的网线，在 OLSS 服务器上仍然能看到 6577 端口的连接，不同的是从 TS 服务器从计算机名变成了 IP 地址（如图 4 所示）。再把另一根用于连接办公网的网线也拔掉，用户正是通过这根网线从办公室来连接 TS 服务器的。奇怪的是，在 OLSS 服务器上到从 TS 到 6577 端口的连接仍然存在，而且不停增加，这是哪里出了问题呢？

[illegible]

图 4 OLSS 服务器 netstat 显示端口连接 b

查看了 OLSS 服务器上的日志，只有一个网卡网络连接在下午 2:24 有断开的警告记录“Broadcom BCM5709C: The network link is down. Check to make sure the network cable is properly connected”，也就是停电那会儿，应该是机房这台交换机未接入 UPS 电源所致，而且在每两周重启服务器也会有这么一条日志。

把显示器键盘鼠标再次切到 AIC 服务器上运行 OpenLAB 程序，这次没有显示一直在连接的状态，而是马上报出错误提示“Connection to Shared Service failed”(如图 5 所示)。这是问题测试检查有进展的标志，说明之前程序启动时一直处于连接状态确实和 TS 服务器大量连接到 OLSS 服务器的 6577 端口有关，导致其无法及时响应 OpenLAB 程序的连接。



图 5 OenLAB 软件启动直接报错

综合分析觉得，问题是出在 OLSS 服务器，可是这个服务器在停电那十多分钟都是正常在运行，怎么回出现这么奇怪的问题呢？更奇怪的是上次停电出现的类似故障居然自动恢复了。难道真得用重启 OLSS 服务器的大招吗？

看着 AIC 上面程序启动时报的错误提示，忽然想到就重启下安捷伦的相关服务看行不行。立即运行“services.msc”，找到一个和错误提示类似的服务“Agilent OpenLAB Shared Services”，重启服务很顺利地完成了（如图 6 所示）。再次去 AIC 上运行 OpenLAB 程序，很快出现了熟悉的登录界面。让实验室的同事登录进去查一下加班运行的仪器情况，很遗憾仪器没有配 UPS 断电就停止运行了，上午所做的几个分析试验得全部重来。



图 6 软件报错相关服务

将刚才断开的 TS 两条网线按标记顺序接上，实验人员就可以正常从办公室连计算机接到远程桌面操作仪器了（如图 7 所示）。

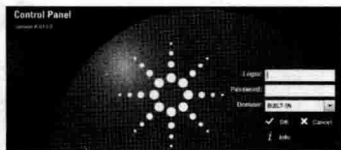


图 7 OpenLAB 软件正常启动界面

最后将上述处理截图发邮件给直接联系的厂商售后工程师，请教出现此问题的更深层次原因，从而避免此类故障给公司造成工作上的损失。还没等到厂商回复的故障原因，不到一周时间又接到供电局通知，说周五 12:30 到 14:00 “将有两次短时停电，每次 3 到 5 秒”，这次试验室的同事和我们商量决定，在 4 台 AIC 服务器所连的仪器上做个测试样，以确认更具体的情况。就这几秒的停电真让信息系统受不了，结果是只有一台 AIC 服务器上的分析测试运行正常，这下得深入分析对比一下各服务器 Windows 日志和网络连接问题了。

远程登录 AIC，发现有两台有非正常关机的提示，也就是说这两台服务器在几秒的断电过程中自动重启了。仔细想想这两台是后来添加的，当时电源插线板孔位不够就再串接了一个，串接时可能接到市电的电源插

座上了，平常没感觉，这几次断电才知道错误了。由于之前接服务器的网络未作详细标识，网络机柜又装着 6 台交换机，实在不方便找出某个服务器接哪台交换机几号端口，还好都是可配置的 H3C 交换机，用笔记本电脑连接控制口执行“dis mac-add”将端口对应学习到的 MAC 地址表复制下来，再比较各服务器网卡的物理地址，终于找到网络连接的端口。有 4 台服务器 Windows 日志里在停电时出现了网络连接断开的警告记录，均连接到第一台交换机上，说明此交换机也没有接入 UPS 电源，和同事确认这台机器后来为了测试整个系统反应慢的问题，而增加的全千兆交换机，没有接入 UPS 电源。

找到问题根源，处理就好办了，同时也发现前几次 OLSS 服务器上的“Agilent OpenLAB Shared Services”服务异常是其网络连接断开所致。

经验总结

如果我们直接重启服务器当然也能把问题解决，但那样做并不能让我们找到问题的更进一步原因，而当某些情形不容我们去慢慢分析时，重启服务器确实也是有效的常用大招。经过此番探研，下次再出现类似问题，我们不必使用重启服务器的大招，也能精准快速解决问题，经验就此积累。通过此次问题的深入排查，也暴露了我们在后期更新维护过程中不规范作业，机房服务器和交换机本应接 UPS 电源系统居然出了差错，每次遇到停电，大家都还理所当然地认为机房里设备都有接入 UPS 电源呢。

图像编码器互联故障解析

辽宁 高大伟

故障现象

单位前期环境安全监控建设完成后，视频图像一直传输正常，近期值班人员反映下级单位的前端图像的时间已经停滞，表明图像已不能正常传输。

故障排查

视频图像的传输链路比较简单，前端图像经编码器编码后，经过集线器与接入交换机互联，然后传到本单位值班室经解码器解码传到监控电视。

首先想到的是图像编解码器长时间开机出现死机后引起的, 但将图像编解码器重启后, 图像依然不正常。其次怀疑是两个单位的网络不正常, 在本单位可以 Ping 通下级单位的网关, 但 Ping 不通下级单位的图像编码器, 初步分析是下级单位的图像编码器故障。

到了下级单位后, 笔者将笔记本接到集线器上, Ping 图像编码器, 时通时断, 但 Ping 上级单位的图像解码器是正常的, 而直接将网线直连图像编码器, Ping 就正常。起初笔者怀疑是集线器的问题, 但替换集线器后, 故障依旧。难道网线有问题? 但下级单位有两台同型号的图像编码器, 故障现象是一致的, 网线同时出问题的概率还是很低的。笔者换了一根网线, 故障依然存在。

集线器、网线、图像编码器都正常, 故障点在哪里呢? 既然 Ping 图像编码器时通时断, 会不会是集线器存在环路呢? 笔者试着将集线器的网线逐根拔下来, 当拔到一根时, Ping 图像编码器竟然正常了。笔者以为已经锁定了故障点, 但下级单位值班人员却说前端图像停滞了。赶紧 Ping 上级单位的图像解码器, 居然也 Ping 不通了。由于下级单位连接的网线比较乱, 费了半天劲才将刚拔下的线查明白, 原来这根线是与接入交换机连接的, 赶紧将它恢复。

问题查到这, 才意识到前面的排查走弯路了, 这次故障点可能与接入交换机有关。由于起初以为故障比较简单, 因此并没有同下级单位网管人员沟通, 现在看来

下级单位的接入交换机存在问题。电话与下级单位网管人员了解, 了解到前期下级单位基于网络使用安全的考虑, 在接入交换机作了网络地址过滤。由于图像编码器为笔者单位配发给下级单位, 而下级单位网管人员对此并不知情, 因此将图像编码器使用的网络地址过滤了。

故障排除

找到了故障产生的根源后, 下级单位网管人员重新配置地址过滤列表, 将图像编码器使用的网络地址添加到允许的范围内, 图像恢复正常。

经验总结

图像的网络传输作为网络的一种应用, 依赖于基础网络的正常运行。随着网络链路串接的设备不断增多, 故障点也随之增加。在应用出现故障时, 首要的是排除应用设备的故障, 然后通过分段排查基础网络的原因。其次在与外单位协同排查故障时, 必须与其技术人员沟通, 尽量了解近期设备运行及配置改动情况。总之, 网络应用若出现问题, 网络技术人员要运用原理性的知识理解工作中出现的问题, 只有如此才能为网络应用可靠运行提供有力的技术支撑。

❖ 添加带外控制设备网不通

故障现象

笔者单位近期进行了卫通中心站和端站的扩容建设, 从卫星通信可靠性的角度考虑, 为卫通中心站和端站购置了带外控制设备。卫通中心站和端站的连接关系如图 1 所示。

▼ 辽宁 高大伟

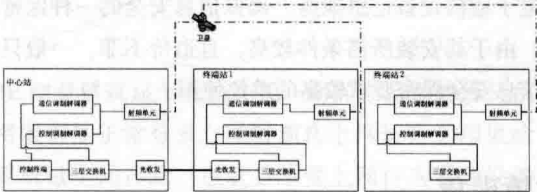


图 1 卫通中心站和端站的连接关系图

终端站 2 和终端站 1、中心站分别通信, 两条链路互为备份, 终端站 1 在中心站附近, 两者通过光收发互

联。设备安装配置完毕后,中心站控制终端站 2 没有问题,但中心站与终端站 1 的控制端始终无法连通。

故障排查

由于链路涉及的环节较多,因此需按照分段排查的思想处理故障。首先,将终端站 1 的控制调制解调器放在中心站三层交换机上,两者可以连通,说明终端站 1 的控制调制解调器没有问题。其次,将一台笔记本电脑放在终端站 1 的三层交换机上,与终端站 1 的控制调制解调器也能连通,说明终端站 1 的网络连接没有问题。用这台笔记本电脑与中心站的控制终端相互 Ping 包,也可以连通,说明中心站与终端站 1 的网络没有问题,但笔记本电脑始终无法 Ping 通中心站的控制调制解调器。笔者初步判断问题出在控制调制解调器上。

故障分析

在笔记本电脑上启用抓包软件,通过分析发现,当笔记本电脑 Ping 中心站的控制调制解调器时,虽然能发现控制调制解调器的 MAC 地址,但始终无法解析为 IP 地址,因此两者始终无法通信。

故障排除

找到了故障根源后,怎么解决 MAC 地址无法解析的问题呢?笔者研究了一下三层交换机,发现交换机并没有启用三层协议,即当作一个集线器使用,工作在二层。既然控制调制解调器在二层无法解析 MAC 地址,是否可以启用三层协议,在网络层完成通信呢?笔者在中心站和端站 1 的三层交换机划分了一个 VLAN,并为 VLAN 配置了 IP 地址,将中心站和端站 1 涉及到带外控制的设备都接到这个 VLAN 里,中心站和端站 1 的控制设备可以连通了,通过抓包软件可以看到 MAC 地址可以解析了。经过一段时间拷机,设备工作稳定,故障排除了。

经验总结

如今,信息传输链路串接的设备不断增多,故障点也随之增加。在信息传输链路出现业务故障时,首要的是以分段的思想排除可能的疑点,不断缩小故障点,直到确认故障原因。总之,信息传输链路出现问题并不可怕,只要有了思路,困难必定迎刃而解。

电磁屏蔽机房维护记

江苏 蒋磊

电磁屏蔽机房是利用“法拉第笼”原理,通过由金属制成的屏蔽体,将电磁波局限于某一范围内,从而阻止电子通信设备信息泄露,确保信息安全的一种保密设施。由于其安装所需条件较高,且造价不菲,一般只在对信息安全保密要求较高的单位使用。

故障现象

笔者所在单位使用的屏蔽机房建于 2012 年,主体材料采用冷轧钢板焊接而成。在最近一次机房屏蔽效能

例行检测中,按照 GJBZ-20219-94 标准,所取的测试点有一半达不到军用 C 级标准,合格参考值为 85db,有的点甚至只有 60db,屏蔽效能较上一次检测大为降低。

故障排查

屏蔽效能不达标,就意味着电子信息随时有被窃取的可能。保密部门通知限期整改,由于厂家较远,且已过保,笔者与同事先对机房进行了整体外观检查,但未发现明显损坏,所有钢板焊接处完好,放置各类

强弱电电缆的滤波器，以及通风波导窗和波导管外观也完好无损。

问题到底在哪？笔者再次查阅了检测报告，发现不合格的检测点多数分布在机房门附近，该门采用的是铰链式插刀门，是机房惟一可以活动的部件。经深入查看，在门框四周的铜质弹簧片深处，发现了很多绿色的铜氧化物，即铜锈，门体上的刀槽和弹簧片也有严重的氧化，门框两侧和下方的镀铜磨损严重。回想起夏季，机房门经常有“出汗”现象，难道罪魁祸首就是锈蚀和磨损？

此时，厂家人员的检查也证实了笔者的判断，正是因为门体与门框导电部位的锈蚀和磨损，导致电流无法正常通过门体和门框，从而无法形成完整的“法拉第笼”。同时发现门体也有轻微扭曲变形，这导致关闭门时，刀槽和弹簧片无法达到紧密的接触，两者作用相叠加，屏蔽性能自然下降。

故障解决

找到了问题的结症，笔者立即会同厂家制定并实施了处理措施，包括更换全部弹簧铜片、门体门框刀槽处除锈、重新喷镀铜及门体矫正，再次申请复测，所有检测点数据均达标。

经验总结

1. 要做好屏蔽机房壳体尤其是机房门的防潮防锈措

施。门是机房惟一可活动的部件，更是综合屏蔽效能的关键。在气候湿润地区，尤其在梅雨季节，必须定期对门体门框进行检查，保证金属导电部分保持干燥。可以定期喷涂“奥大林”除锈润滑剂，能有效减少锈蚀。夏季，机房内空调温度不宜太低，否则会导致门内外温差过大，形成冷凝水，产生锈蚀。

2. 尽量减少机房门的开启。屏蔽机房门可分为铰链式插刀门、平移门两大类，前者外观和普通门类似，因自身重量较大，如长期处于开启悬挂状态，矩形门体的一侧会因重力作用而下垂变形，从而导致刀槽口和弹簧片不能紧密贴合。同时，开门过多也会人为增加门框导电层的磨损。

3. 要做好机房内设备与滤波器等通道的位置规划。机房里设备众多，除了放置服务器、网络设备的机柜，还有精密空调、UPS 电源柜等。这些大型设备位置一旦确定好，很难挪动。而滤波器、波导管、波导窗也是影响屏蔽性能的短板。建议机房内大型设备与上述通道保持一定距离，以方便排查故障。

4. 要定期对机房屏蔽效能进行检测。专业的屏蔽机房检测设备非常昂贵，且很难购买。市场上有一种简易的屏蔽设备检漏仪，外形类似对讲机，使用也很简单。保密无小事，千万不要等到出现问题才去补救，维修费用昂贵是一方面，一旦造成信息泄露，那就不单单是钱的问题了。

❖ 360 浏览器医生排除故障

广东 赖文书

搞定 IE 浏览器无法登录网银账户

同事处理财务计算机无法登录网银账户，先以为是受上网行为管理影响，于是在深信服 AG-6700 上把该计算机 IP 开直通，也就是暂时放弃管制，可是用户问题依旧。到用户处检查其他网站均能正常访问，访问银行网银网站也是没问题，只是在插上 U 盾以证书

登录 IE 浏览器就显示无法连接。而同办公室的另一台电脑网银都能正常登录。此时想在上网行为管理里给该计算机做全局排除，也就是不受上网行为管理设备的任何影响。

这时输入 `https://192.168.99.2` 却无法显示控制台页面，难道该网段无法访问上网行为管理设备？Ping 设备 IP 是完全正常，再输入 `http://192.168.99.2` 却

能正常显示用户验证页面。这就奇怪了,不能登录银行网银账户,会不会是因为 https 的关系呢?百度搜索“https 无法访问”。

方法一,取消 Internet 选项→高级选项中 TSL 1.0 前面的勾,记忆中以前好像遇到过这种情况,可是今天这里无效。方法二,重置 IE 浏览器设置,点击 Internet 选项→高级选项重置按钮没反应,本来应该弹出确认框“在重置 Internet Explorer 设置之前,必须首先关闭所有打开的窗口和程序”,此时怀疑 IE 浏览器真有问题。方法三,运行“net start cryptsvc”命令启动与 SSL 有关的服务,使用 regsvr32 命令依次注册相关的动态链接库文件,传说中处理此问题的绝招,此时似乎仍然不奏效。

最后安装 360 安全浏览器 7.1,不管是使用 IE 模式还是极速模式,结果都一样的让人绝望。突然想到以前用过其自带的浏览器医生解决了很多疑难杂症,经过多次版本升级这个小工具已经变了模样,不过仍然在状态栏的位置。轻点鼠标三下,弹出“浏览器医生修复需要关闭安全浏览器,是否关闭以继续修复?”对话框,继续退出浏览器自动进行修复各选项(如图 1 所示),完成后再次插入银行网银的 U 盾,启动浏览器就正常进入了网银账户,再次 IE 访问 https://192.168.99.2 也没有问题了。两个人弄了一个多小时也未搞定的问题,浏览器医生分分钟搞定。

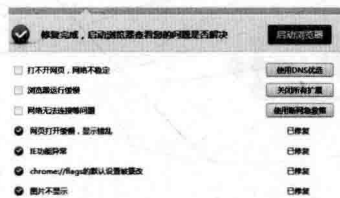


图 1 浏览器修复医生

12306 订票网上支付报错

登录 www.12306.cn,按网站说明下载安装好根证书,预订火车票一切顺利。就在最后一步“网上支付”时,跳出了错误页面提示:交易失败,代码:50050,描述:交易信息不完整。

会不会是网站问题呢?咨询 12306,对方称网站正常此种情况是网络不稳定,退出再进入操作就可以。得到官方答案满怀希望地试了几次关闭浏览器重新登录 12306,依然是无法网上支付。

在百度搜索“12306 支付出错交易信息不完整”,有位网友的博客以 IE9 图文并茂的描述了该问题的解决办法,将 https://*.12306.cn 加入 Internet 选项安全里的“受信任的网站”,翻了好几页的搜索结果全都是这种解决方式,可是在我的 IE8 和 360 安全浏览器里均不见效,IE 倒是出现了和 360 浏览器不同的报错页面“Internet Explorer 无法显示该网页”。

换了一台电脑,以 Chrome 浏览器登录进行网上支付,跳出了正常的支付方式选择页面,一路操作下去居然顺利完成了。难道是我的电脑有问题?想到了上次用浏览器医生解决了登录网银的疑难杂症,本来就是用的 360 安全浏览器为什么没首先想到试试它呢?分分钟又终结了我折腾一个多钟头的故障排查。由于自己还管理着防火墙和行为管理设备,期间试过调路由走不同外网出口、行为管理全局排除等动作,真是乱了处理问题的阵脚。

经验总结

两个问题的操作系统前一个是 Windows XP,后一个是 Windows 7,由于工作原因均使用了超级管理员组的权限,使用过程不经意间使 IE 组件受损,导致奇怪的浏览器问题。普通用户下的系统还是很少遇到这些疑难杂症,最小权限原则在用户计算机管理也是相当有用的。处理终端网络问题,除了观察分析错误现象外,首先需要和其他终端对比,以确认问题网络方面的还是终端方面的,再诊断确认是应用程序的还是更下一层系统组件的问题。遇到计算机系统问题网上搜索很重要,能快速找到一些别人类似问题解决方法和思路,毕竟我们平时对系统深层组件接触认识有限,但是借助一些小工具更能让我们在解决问题中事半功倍。

或许是我用其他浏览器少,不知道其辅助工具的功能,360 浏览器医生确实很好用,更深层次的功能还需要借助“断网急救箱”或者“安全卫士”等产品支持(如图 2 所示)。

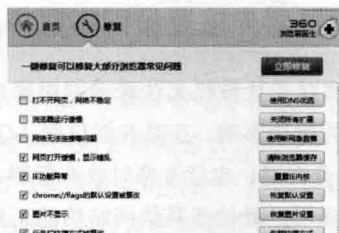


图 2 断网急救箱

网关 IP 配置引发故障

江苏 王旭

近日，市教育城域网改造，将原有的 VPN 模式改为裸光纤模式，每个学校新增一台锐捷路由器和深信服防火墙。原有的光纤猫更换为光模块直连。电信工程师根据他们拟定的改造计划配置设备，发现故障不断，经过大家共同多次调试，最终发现原来是电信设计的 IP 配置问题，后来根据锐捷的规范，问题得以顺利解决。

电信工程师到我校直接按照他们设计的参数进行配置。首先给大家介绍下我校的网络拓扑结构。学校原有网络拓扑是，网关锐捷 EG-1000S，外网口 10.20.80.122/28，内网口 1.1.1.2/24。核心 RG-8606，地址 1.1.1.1/24，划分 VLAN64 ~ VLAN75，VLAN 地址分别为 10.21.64.254……10.21.5.254，网络拓扑结构如图 1 所示。



图 1 原有校园网络拓扑结构

故障现象

工程师根据设计方案，将路由器外网口配置为 10.20.80.122/28，内网口 10.21.79.254/24。网关外网口配置为 10.21.79.253/24，内网口保持 1.1.1.2 不变，拓扑结构如图 2 所示。把网线插上，发现当配置线插上网关 Control 口登录时，笔记本终端明显反应卡顿，屏幕命令行每隔一段时间连续跳出 no radius 的提示，给配置带来很大的干扰。但是在配置终端测试连接是正常的，从网关到路由器是通的，从核心到网关也是通的，内网用户到核心是通的，网页却打不开。再经过测试，从客户端到网关不通，从核心到路由器不通。工程师

开始搞不懂，表示从未遇到过这种现象，抱怨锐捷的设备问题。

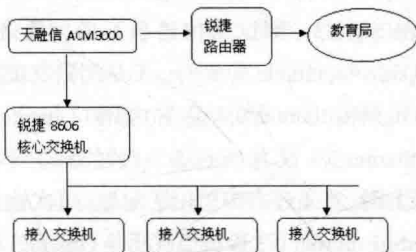


图 2 教育局规划的拓扑结构

故障排查

仔细研究他们的设计方案，我想起今年 5 月份一起配置 VPN 的经历，当时由于校领导想通过登录校内网，连接教育局的办公系统，尝试开启网关 RG-1000S 的 SSLVPN 功能，配置隧道地址 10.21.64.8，因为 10.21.64.8 是城域网公网地址的映射，开启 SSLVPN，这时发现内网用户不能上网了，客户端与核心 RG-8606 通讯正常，与 RG-1000S 不通。仔细分析网络拓扑，发现逻辑上没有问题。于是用设备 RG1000S Control 口登录，将 SSLVPN 关闭，去掉 10.21.64.8 隧道地址，这时候网络一切正常。

没办法，致电锐捷客服，技术支持解释网关不可以用内网地址，如果要用 VPN 需要增设一台 VPN 设备放在内网。当时也是愕然，锐捷设备还有这个规则。当时觉得不划算，就直接在 Windows 2008 下面做了 VPN。回想这件事情，今天的问题应该也在这儿。

内网地址不可以出现在网关中，应该也不可以出现在网关的上一层。于是建议现场工程师重新配置，现场工程师致电锐捷技术支持，锐捷工程师了解情况后，让现场工程师拿掉路由器，似乎锐捷工程师也不愿解释，现场工程师表示很无奈。现场工程师将路由器光模块插到网关 1F 光模块插槽，发现光模块灯不亮，

怀疑该接口为光电复用接口。再次致电锐捷技术，解释光口 1F 和 g0/1 是光电复用口。可是，当前 g0/1 配的地址是 1.1.1.2/24，无奈将 1.1.1.2/24 配到 g0/3 口，g0/1 接口模式设置为光口。现在地址配置好了，测试发现网络还是不通。

故障解决

仔细查看，发现网关的路由表后面跟着接口地址默认路由 0.0.0.0 0.0.0.0 1.1.1.2 后面跟着一个接口地址 GigabitEthernet 0/1，于是将 GigabitEthernet 0/1 更改为 GigabitEthernet 0/3，测试结构还是不通。我猜想接口估计有 inside 和 outside 配置的，于是配置发现果真，将接口 GigabitEthernet 0/3 设为内网口 inside，接口 GigabitEthernet 0/1 设为 Outside。经过测试，内部用户还是不能上网。难道还有哪里出了问题。再次检查配置，发现 GigabitEthernet 0/3 接口模式还是 Outside，很不解，明明设置好了且保存了呀。再修改，保存，用内网用户测试，终于好了。

经验总结

到这里，大家都没有成功后的喜悦，感觉本来应该是很简单的工作，但操作完很辛苦。工程师感叹今天真的学到了很多锐捷的知识。通过这件事情，我想并不是这位工程师的水平不够高，可能他对锐捷的设备接触的比较少，锐捷设备的通用性上面还是有缺陷，是多一份经历多一份经验罢了。锐捷设备凭借较高的服务质量，在教育部门的占有量越来越多，作为教育部门的工程师要多了解身边设备的特性与短板。也希望锐捷在做好服务的同时，在产品通用性上多下功夫，相信可以在一定程度减轻工程师的工作量。图 3 是完工后的网络拓扑图。

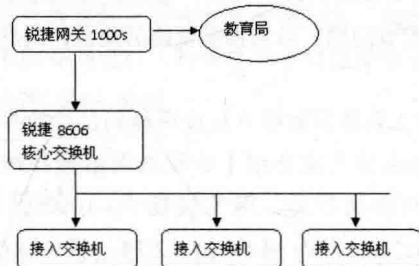


图 3 完工后的网络拓扑结构

IRQ 冲突硬件无法使用

福建泉州 王刚 郑洪飞 荣世辉

故障现象

在为一台组装计算机安装 Windows 系统并正常安装硬件驱动后，使用 USB 无线网卡可以正常上网，在 USB 接口插入手机，并为手机启用 USB 模式，无线网卡出现断线现象。通过查看设备管理，发现原来无线网卡和手机出现硬件冲突，在手机插入其他几个 USB 接口后，无线网卡仍然无法恢复正常。用鼠标右键点击“我的电脑”依次选择“管理→设备管理器”，在界面中发现有硬件出现黄色的“？”。

故障分析

在本操作中，硬件驱动程序安装正确，但在插入手机后，手机 USB 模式占用了原有本属于 USB 无线网卡的中断请求（IRQ）线路、直接存储器（DMA）通道和输入/输出（I/O）端口及内存地址等计算机资源，当将相同的系统资源分配给两个或多个硬件设备时，就会在硬件之间发生资源冲突，造成导致 USB 无线网卡无法正常上网。

IRQ 家族

所谓 IRQ (Interrupt Request) 意为中断请求, 是硬件设备向 CPU 发送一个中断请求, 以获得 CPU 的服务响应。在早期使用的计算机中, 是由一个中断控制器 8259 或 8259A 的芯片来控制操作系统中每个硬件的 IRQ 值, 共有 16 组 IRQ, 因芯片本身需“桥接”使用一组 IRQ, 实际上只有 15 组 IRQ 可供硬件使用。这 15 组 IRQ, 在 BIOS 中通常都有自己所对应的硬件设备, 每一种类型的硬件设备原则上都会有一个不同的 IRQ。正常情况下, CPU 是处于不间断的工作状态, 而当某一个硬件设备开始或结束收发数据, 需要 CPU 处理数据运算时, 便使用其 IRQ 对 CPU 送出中断请求讯号, CPU 会暂停当前工作, 先行处理这个硬件响应, 这便是中断请求的作用。根据日常使用要求和习惯, 很多 IRQ 均固定使用, 只有部分会闲置。

硬件设备的 IRQ 信号由中断控制器 8259 或 8259A 的 INT 引脚输入到 CPU 的 INT 引脚去申请, 这是一个 8 位的二进制数 (如图 1 所示)。

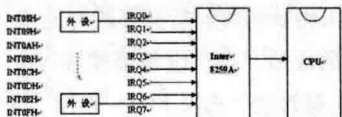


图 1 8259A 控制器

16 个 IRQ 是用 2 个 8259 或 8259A 通过级联来实现的 (如图 2 所示)。

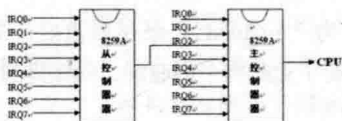


图 2 级联的 8259A 控制器

通常, CPU 会依据 IRQ 优先级来决定响应, 这 16 组 IRQ, IRQ0 优先级别最高, IRQ15 优先级别最低。其优先级由主控制器和从控制器配合形成, 将主控制器上定义为 IRQ0-IRQ7, 将从控制器上的 IRQ0-IRQ7 定义为 IRQ8-IRQ15。

IRQ 的分配

从 Windows 95 操作系统开始, Windows 操作系统开始应用“即插即用”(PNP)技术, 计算机所有 IRQ、DMA 通道和 I/O 端口等系统资源都被操作系统

接管, 并由 Windows 操作系统根据硬件情况进行自动分配。在较早的 Windows 操作系统或较早的计算机主板上, 由于 IRQ 资源数量有限, 因此很多设备往往会共用一个 IRQ, 由 Windows 操作系统的智能分配, 一般都能正常工作。

在操作系统中, IRQ 是由 ACPI (高级配置和电源接口) 或 APIC (高级可编程中断控制器) 来控制的。ACPI 模式为较早的控制模式, 最多只能提供 16 个 IRQ, APIC 却可以提供更多的 IRQ, APIC 是利用装置扩充组合用来驱动 Interrupt 控制器, 每个 CPU 都拥有各自的 APIC, 目前在 Intel 系列的 CPU 中均包含了 APIC 系统, 系统中可拥有 8 个 APIC, 由它们收集来自各类硬件设备的 Interrupt 信号, 每个 APIC 有自己专有的 IRQ 号码。目前主流的单核 CPU 支持 24 个以上输入, 多核 CPU 则拥有上百个 IRQ。

使用 APIC 功能, 必须选用 Windows 2000 以后的操作系统并且主板支持 APIC 模式。

IRQ 冲突

PNP 技术也存在一定的缺点, 即如果不能认出新安装的设备, 那么自动分配中断时就会产生冲突, 特别是在组装计算机中体现尤为明显, 一般为 PCI 网卡、显卡和 ISA 设备设备会产生 IRQ 冲突。正常 USB 设备不存在 IRQ 冲突的问题, 因为它会单独使用自己的保留中断, 因此不会与 PCI 或 ISA 设备去抢夺有限的 IRQ 资源。而当今这个信息时代, 新的硬件设备层出不穷, 很多设备功能相似, 这就导致 Windows 操作系统不能及时正确检测出新设备, IRQ 冲突也就不可避免。

故障排查

确保冲突硬件设备的驱动安装正确。

1. 启动 APIC 模式

进入 CMOS 模式, 选择 Advanced CMOS Features, 修改 APIC Mode 为“Enabled”。

2. 更换插槽

如果仍出现 IRQ 冲突, 可将冲突的硬件更换其他插槽以避免 IRQ 冲突, 采取这种方法时, 需要用户掌握主板 CMOS 默认状态下的 IRQ 资源分配情况, 然后在此基础上调整板卡的位置, 从而避开 IRQ 冲突。

3. 查看冲突设备的 IRQ 中断号

第一种方法：鼠标右键单击“我的电脑”，选择“设备管理器”，在“查看”菜单栏中，点选“依类型排序资源”，在主界面可以看到“中断请求（IRQ）”，就可以看到 IRQ 的使用情况了（如图 3 所示）。

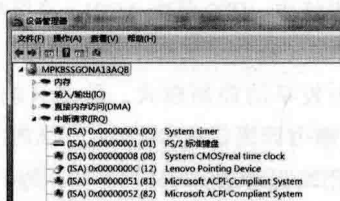


图 3 设备管理器中的设备 IRQ

第二种方法：在操作系统“开始”菜单中，依次展开选择“所有程序→附件→系统工具”或在“运行”对话框中直接输入“msinfo32”。

在“系统属性”的“设备管理器”选项卡上，双击冲突设备，然后在“资源”选项卡上，查看“冲突的设备列表”，确定哪些资源设置与该设备冲突。

4. 禁用冲突硬件

如果发生冲突的设备已不再需要，可以将其禁用，以解决硬件冲突问题。如果禁用即插即用设备，那么，其他设备可自动获取这些设备的资源。如果禁用的设备不是即插即用型，那么必须从“设备管理”的硬件列表中删除此设备，然后将它从计算机中取出以释放所占用的资源。在“系统属性”的“设备管理器”选项卡上，双击要禁用的设备。在“资源”选项卡上，如果能发现“手工设置配置”按钮，则表明该设备能够“即插即用”。

5. 手动分配 IRQ

进入 CMOS 在 PnP / PCI Configurations（即插即

用与 PCI 参数设置）中将“Resources Controlled By”中设置为“Manual”，然后对检测到的硬件的 IRQ 进行重新分配指定后故障排除。

6. 提高冲突硬件的 IRQ 优先值

在故障仍无法排除时，可以提高冲突硬件的 IRQ 优先值。运行注册表编辑器 regedit32，找到注册表中的 HKEY_LOCAL_MACHINE\System\CurrentControlSet\Control\PriorityControl 位置。建立一个名为 IRQ*Priority（其中“*”是具体的 IRQ 中断号）的 DWORD 双字节值，然后把它的值设为 5。例如，系统 CMOS 实时钟的 IRQ 中断号是 9，建立的键名就是 IRQ9Priority，重新启动计算机之后，冲突的硬件 IRQ 的优先值就会提高。

故障解决

笔者遇到的故障问题，手机连接计算机后导致无线网卡中断，刚开始怀疑是驱动的问题，对主板驱动和无线网卡的驱动进行了升级和重新安装，操作系统重启后问题未得到解决。后又怀疑可能是 USB 接口供电不足造成的故障，在“设备管理器”中“USB Root Hub”的“电源管理”选项卡中，去掉“允许计算机关闭这个设备以节约电源”前的勾选和通过 BIOS 设置对 USB 的供电电压进行了调整，问题仍未得到解决。后通过“设备管理器”才发现是 IRQ 冲突所致，进入 CMOS 模式，选择 Advanced CMOS Features，修改 APIC Mode 为“Enabled”，保存后重启，进入操作系统后重新安装了无线网卡的驱动，问题得到解决。

❖ 解析交换机 CPU 占用率

福建泉州 王刚 赖文鑫 叶伟

交换机 CPU 占用率是指一段时间内 CPU 执行代码的非空闲时间与时间段总长度的比率,可反映某个时间段交换机 CPU 资源使用情况,其计算公式为: $\text{CPU 占用率} = (\text{总时间} - \text{空闲时间}) / \text{总时间}$ 。空闲时间是指 CPU 运行 Idle 任务的时间,Idle 任务是一个低优先级任务,不完成具体工作,如果 Idle 任务得到了调度,就认为 CPU 当前处于空闲状态。系统的 CPU 占用率不是保持不变的,它是随着系统的运行和外部环境的变化而持续变化的。正常状态下,交换机的 CPU 占用率不会超过 5%,交换机在采用堆叠方式,其 CPU 占用率不会超过 8%,在配置功能较多的情况下, CPU 占用率不会超过 30%,如果 CPU 交换机占用率超过 50% 则视为不正常。

交换机 CPU 占用率高的危害

当交换机 CPU 处理的数据包过多、各类中断请求过多或部分任务进程占用了较长 CPU 处理时间时, CPU 负载就会增加,无法及时调度其他任务,从而会导致出现业务异常、业务处理能力下降和很多网络故障等。

1. 网络结构改变

一般正常网络环境中,为确保网络不间断工作,会采用备份交换机的网状结构,各交换机同时会启用 STP/SEP/RSTP/MSTP 等生成树功能的协议,避免网络出现环路。在这些协议运行过程中,交换机 CPU 会周期性接收 BPDU 等报文来维持交换机端口 Root/Alternate 等角色,如果交换机 CPU 占用率过高,很可能导致 BPDU 报文不能及时发送和处理,交换机会认为到根桥的路径出现故障,从而重新选择 ROOT 端口,引起网络重新收敛,导致网络拓扑改变。如果交换机原来同时存在 Alternate 端口,交换机会将 Alternate 端口作为新的 ROOT 端口,进行数据收发,导致网络结

构发生改变,也可能导致网络出现环路。

2. Eth-Trunk 主干链路关闭

为提高交换机之间流量带宽,交换机会启用 LACP (链路汇聚控制协议),交换机物理端口在启用 LACP 协议后,会由交换机 CPU 发送 LACPDU 来完成相关汇聚任务,其后链路保活均由 CPU 进行 LACP 协议的计算完成。如果 CPU 占用率过高,就会导致交换机不能及时接收和发送 LACPDU 报文,从而引起 Eth-Trunk 将会链路关闭,造成网络中断。

3. 无法远程管理交换机

远程管理交换机已经成为管理配置交换机的首选方式之一,远程管理和配置一般都是通过 Telnet、SSH、Web 和 SNMP 等协议方式与交换机建立会话来进行。当交换机 CPU 占用率过高时,交换机就无法处理这些会话响应,从而导致无法远程管理交换机,造成管理成本上升。

4. 通过 CPU 转发的报文被丢弃或转发时延增大

当交换机 CPU 占用率过高时,会导致对各类协议控制、组播等报文的转发不及时,交换机内存消耗会增加,从而导致后续协议控制、组播等报文会被丢弃和转发时延增大。需要说明的是,普通数据报文转发由交换机电子集成电路完成,无需 CPU 参与,因此 CPU 占用率高通常并不影响普通数据报文转发。

交换机 CPU 占用率高的正常应用场景

交换机正常运行时, CPU 会处理数以百计的活动系统进程。由于交换机一直处于运行状态,即使无任何业务配置和网络数据包,其 CPU 占用率也不会为 0。在一些应用场景下,交换机长时间运行时, CPU 占用率一般不超过 80%,短时间内 CPU 占用率不超过 95%,可认为交换机状态是正常的。

1. 生成树场景

在交换机应用了 MSTP 协议后, CPU 占用率会同实例个数和活动端口数成正比, 数量越多, 用于计算和维护的 CPU 资源就会增多, 在应用了 VBST 协议后, 由于每个 VLAN 独立运行一个实例, 因此在相同 VLAN 和端口数目下, VBST 会比 MSTP 占用更多的 CPU 资源。

2. 更新路由表

当一台三层交换机接收到路由更新消息时, 交换机会占用 CPU 资源将路由信息更新。CPU 占用率取决于路由更新信息的多少、更新频率、接受路由更新进程数量、堆叠交换机数量等, 路由更新信息越多、更新频率越快、路由更新进程数越多、参与堆叠的交换机数量越多, CPU 占用率就越高, 对于堆叠交换机, 路由信息还需要同步到其他成员交换机。

3. 执行配置管理类命令

部分配置命令需 CPU 长时间参与也会导致 CPU 占用率暂时升高, 这些命令主要有: 用户视图下执行 copy flash:/ 命令、配置内容很多的情况下执行 Save 命令和 Display running-configuration 命令、执行用于输出各类调试信息的 Debug 命令、执行持续时间长且数据包多的 Ping 命令、交换机端口启用了执行 Port-security mac-address sticky 相关命令时、还有利用交换机抓包的命令等。

4. 交换机参与堆叠

在交换机堆叠环境中, 由于主要业务运行在堆叠主交换机上, 还需要周期性维护堆叠成员状态, 因此主堆叠主交换机的 CPU 占用率比单台交换机运行时的 CPU 占用率高, 堆叠成员交换机数量增多时, 堆叠主交换机的 CPU 占用率也会相应升高。

5. 交换机参与堆叠

有较多管理用户同时远程管理交换机时、交换机启动后有较多客户机生成 MAC 地址表时、交换机启用 DHCP 功能有大量 DHCP 请求时、增加数量较多的 VLAN 并将各端口加入 VLAN 中时、交换机端口频繁 Up/Down 时、网络流量增加时等。

故障引发交换机 CPU 占用率高

除正常应用场景外, 只要是交换机 CPU 占用率高, 都可视为故障, 应及时排除。

1. 网络环路

网络环路是造成交换机 CPU 占用率高的最常见最主要的原因。当出现网络环路时, 交换机会发生 MAC 地址漂移, 产生的广播风暴产生大量无效报文, 会消耗交换机 CPU 资源。

2. 网络震荡

网络震荡也是导致交换机 CPU 占用率的另一大重要原因, 在出现网络震荡时, 网络参数会频繁发生改变, 交换机忙于网络切换事件, CPU 就会增加工作量。

3. 交换机遭到攻击和网络中存在病毒

当网络中存在 ARP 病毒, 交换机遭到 DHCP 攻击、BPDU 攻击、SSH 暴力破解等恶意攻击时, 交换机 CPU 将不得不处理这些报文, 导致 CPU 长时间处理这些攻击报文, 造成交换机 CPU 占用率高, 性能下降, 从而引发其他业务的中断, 影响正常的业务。

4. 交换机部件故障

当交换机部件出现故障后, 部件会发送大量 SRMI、SRMR 等中断报文, 其他正常部件也会发送大量的保活类报文给交换机 CPU 来连通交换机故障部件, 而这些报文都会极大地消耗交换机 CPU 资源, 造成交换机 CPU 占用率高。

5. 配置错误

这里以 VLAN 配置为例进行说明, 实际需要的 VLAN 不多, 但却建立了很多无效 VLAN, 而每建立一个 VLAN 时, 即使没有客户机, 交换机都会发送一条 ACL, 来捕获该 VLAN 中的 ARP 报文, 如果 VLAN 过多, 就会导致交换机 CPU 占用率高, 还有在 GVRP 环境下频繁创建和删除 VLAN, 每发送一条命令, 就会触发大量报文通信, 也会造成交换机 CPU 占用率升高。

CPU 占用率高故障排除方法

当发现 CPU 占用率过高时, 首先要确定 CPU 占用率高是否是正常现象, 除了正常应用场景外, 都可以视为是故障引起, 再进行故障排除。正常的处理步骤为“确定故障现象、判定故障原因、进行故障修复”(因本文中涉及部分交换机操作命令, 本文中所有命令以华为交换机操作命令和功能为例, 其他品牌交换机均有类似命令和功能)。

1. 确定故障现象

可以通过几种方式来确认是什么任务、是什么报文

是和交换机上哪个硬件模块引起的 CPU 占用率高,通过交换机当前任务、报文类型和模块接口可以直接找到在什么接口什么原因造成的故障,确定故障流程如图1所示。



图1 确定故障流程

(1) 获取 CPU 占用任务情况, 确认高比例任务。

在用户模式下, 执行 display cpu-usage 命令, 可以查看各在线任务的 CPU 占用率, 可以记录占用率最高的前3个任务名称(如图2所示), 其占用率排名前3的任务分别是 FTS、VIDL 和 bcmRX。表1为可引起交换机 CPU 占用率高的常见任务名称和功能描述。

```

<Quidway>display cpu-usage [ slot x ]
CPU Usage Stat. Cycle: 60 (Second)
CPU Usage      : 85% Max: 99%
CPU Usage Stat. Time : 2001-04-25 16:15:00
CPU utilization for five seconds: 90% one minute: 85% five minutes: 86%
Max CPU Usage Stat. Time : 2001-04-24 17:17:07.

TaskName      CPU Runtime(CPU Tick High/Tick Low) Task Explanation
---
BOX            0% 0/ dad772 BOX Output
_TIL           0% 0/ 0 Infinite loop event task
EXC            0% 0/ 0 Exception Agent Task
VIDL          15% 8/65168116 DCPRA TASK
TICK           0% 0/ 91e2d7f
CLKI           0% 0/ 0 CLKI
DRV            0% 0/ 12202d9 DRV Device
bcmRX          9% 0/ 638175f bcmRX
CHAL           0% 0/ 0 CHAL
PTS            23% 0/ 5a375 PTS
MCD            0% 0/ 0 MCD Module Management
  
```

图2 交换机当前占用率最高的3个任务

表1 可引起交换机 CPU 占用率增高的常见任务

任务名称	功能描述
VIDL	统计空闲业务的 CPU 使用率
SOCK	IP 协议栈报文调度和处理
RPCQ	提供远程过程调用功能
ROUT	负责各路由协议路由选路以及路由学习, 进行最优路由的选择并下发 FIB
bcmRX	提供从芯片接收报文的功能
FTS	FECD 创建的收包任务, 驱动收到报文后, 若不是超级任务则把报文给 FTS 任务处理
TIL	监控、处理软件异常导致的死循环
ACL	访问控制列表
bcmTX	提供向芯片发送报文的功能
CSSM	实现堆叠协议栈, 管理堆叠状态
INFO	接收、输出业务模块产生的日志、告警
SRMI	外部中断处理任务
VT	虚拟终端任务
VRRP	实现 VRRP 协议栈, 管理协议状态机, 维护协议相关的数据库
STRB	接口板监控与识别攻击流量
STRA	实现监控与识别攻击流量, 并对攻击源进行惩罚的功能
SLAG	实现 E-TRUNK 功能
SECE	实现 ARP 安全、IP 安全以及 CPU 安全等功能, 管理协议状态机, 维护协议相关的数据库信息
PTAL	实现重定向认证功能, 完成认证授权, 管理协议状态机, 维护协议相关的数据库

(2) 获取 CPU 占用率高的模块信息, 确认高比例模块接口。在用户模式下, 执行 display cpu-usage [slave|slot slot-id] 命令, slot-id 在堆叠系统中表示堆叠 ID, 可以查看相关模块占用交换机 CPU 的比例统计信

息(如图3所示), 为交换机 slot 0 模块的硬件 CPU 占用率。

```

<Quidway> display cpu-usage slot 0
CPU Usage Stat. Cycle: 60 (Second)
CPU Usage      : 99% Max: 100%
CPU Usage Stat. Time : 2014-06-05 15:19:46
CPU utilization for five seconds: 99% one minute: 75% five minutes: 42%
Max CPU Usage Stat. Time : 2014-06-05 14:33:36.

TaskName      CPU Runtime(CPU Tick High/Tick Low) Task Explanation
---
ARP            30% 0/6da2823b ARP
RS             30% 0/82a0221f Operation System
L2TF           21% 0/8448f54 L2TF
IFPD           8% 0/1e070990 IFPD Ifnet Product Adapter
L2_P           3% 0/1a77752b L2_PR
FTS            2% 0/13e06e3e FTS
IPCQ           2% 0/1256ab6f IPCQIPC task for single queue
STP            2% 0/175350b9 STP
VPR            2% 0/16254e6f VPR VP Receive
sv_rx7         2% 0/123d908c sv_rx7
VIDR           1% 0/ 5f5d76f VIDRRA INLE
mv_rx6         1% 0/ db73d34 mv_rx6
  
```

图3 子模块占用交换机 CPU 的比例统计信息

(3) 获取 CPU 占用率高报文统计信息, 确认高比例报文类型。在用户模式下, 执行 display cpu-defend statistics all 命令, 查看上送 CPU 报文的统计查询信息, 获取报文类型, 特别要关注丢弃计数(如图4所示), 通过各类协议的 Drop 计数来确认是否存在冲击情况, 如果某类协议存在的 Drop 数很大, 则可以认为该协议存在冲击 CPU 情况。

```

<Quidway>display cpu-defend statistics all
Statistics on slot 0:

Packet Type      Pass(Bytes) Drop(Bytes) Pass(Packets) Drop(Packets)
---
arp-miss         0 0 0 0
arp-reply        384 0 6 0
icmp-request     346825664 83619584 5419131 1306056
dhcp-client      0 0 0 0
dhcp-server      1427 0 4 0
dhcpv6-reply     0 0 0 0
dhcpv6-request   0 0 0 0
icmp             0 0 0 0
icmpv6           0 0 0 0
igmp             2240 0 35 0
  
```

图4 各类协议 Drop 数量

2. 判断故障原因

依据收集到的各类信息, 判断故障产生的原因。

(1) 系统类原因。系统主要是对交换机中各部件进行管理, 同时给其他业务和模块提供系统基础支持。系统类问题主要是操作系统本身故障和模块故障触发, 操作系统故障一般是硬件故障或操作系统故障, 模块类故障一般是模块硬件故障和配置原因, 通常表现为 SRMI、SRMR、BCMDPC 等中断处理相关的任务占用率较高, 因此, 如果出现系统 CPU 占用率较高且以上相关任务占用率排名靠前的情况, 则可以判定为系统类故障原因。

(2) STP 震荡原因。使用 display cpu-defend statistics all 可以得到各报文的统计值, 各类报文统计是交换机启动后各类报文收发的总和, 所以在交换机 CPU 占用率高的情况下, 需隔一段时间运行一下这个命令, 这样才能确保单位时间采集到的各类报文统计比较精确。可以通过 display stp topology-change 命令查看 STP 拓扑变化信息来判定是否是 STP 震荡原因,

可以通过执行 `display stp tc-bpdu statistics` 命令查看端口上接收到的 TC-BPDU 统计, 以确定 TC 报文的来源物理接口。

(3) 路由协议原因。这里以 OSPF 协议为例, 可以通过日志查看 OSPF 邻居状态 Down 的原因。执行 `display logbuffer` 命令, 查看日志信息 (如图 5 所示): 其中 `NeighborDownImmediate reason` 关键字记录的是 OSPF 邻居 Down 的原因, 具体原因见表 2。

```

OSPF/3/NEB_DOWN_REASON:Neighbor state leaves full or changed to Down.
(ProcessId=[USHORT], NeighborRouterId=[IPADDR],
NeighborAreaId=[ULONG], NeighborInterface=[STRING], NeighborDownImmediate
reason=[STRING], NeighborDownPrimeReason=[STRING],
NeighborChangeTime=[STRING])

```

图 5 交换机日志信息

表 2 OSPF 邻居 Down 的原因

原因	解释
Neighbor Down Due to Inactivity	表示在 deadtime 时间内没有收到 Hello 报文导致 OSPF 邻居 Down。
Neighbor Down Due to Kill Neighbor	表示因为接口 Down、BFD Down 或执行了 reset ospf process 操作。此时，可以通过查看 NeighborDownPrimeReason 字段判断具体原因。
Neighbor Down Due to 1-Wayhello Received 或 Neighbor Down Due to SequenceNum Mismatch	表示因为对端 OSPF 状态首先变成 Down，从而向本端发送 1-Wayhello，导致本端 OSPF 状态也变成 Down。

(4) 环路类原因。当交换机未启用生成树协议就有可能形成环路，报文会在多个接口间转发，导致 CPU 占用率上升。使用 `display current-configuration`，查看是否使能了 MAC 地址漂移告警功能，如果使能了该功能且存在 MAC 地址漂移现象，就会出现告警信息，如果未使能该功能，可在用户模式下执行 `loop-detect eth-loop alarm-only` 命令，当有 MAC 地址漂移时，就会有告警信息。如图 6 所示，是交换机中有环路，其中 MAC 地址为 0000-0ca8-0101 的地址发生了漂移，漂移分别发生在 GigabitEthernet1/0/3 和 GigabitEthernet1/0/2 端口。

```
Feb 22 2011 18:42:50 Quidway 12T1PPI/4/MC_FLAPPING_ALARM:01D
1.3.6.1.4.1.2011.5.25.42.1.7.12The mac-address has flap value
0.126100.0, entPhysicalIndex=0, BaseTrapSeverity=4, BaseTrapProbableCause=649,
BaseTrapEventTyp=1, MacAddr=0000-c0a8-0101, vlanid=100,
FormerIfDescName=GigabitEthernet1/0/3, CurrentIfDescName=GigabitEthernet
1/0/2, DeviceName=Quidway)
```

图 6 MAC 地址漂移告警信息

此外，如果交换机无法远程登录、在交换机上占用 `display interface` 命令查看接口统计信息时发现接口收到大量广播报文、占用串口登录交换机进行操作时，操作比较慢、通过 `Ping` 命令进行网络测试时，丢包严重、交换机上发生环路的 VLAN 的接口指示灯频繁闪

检测后,交换机出现环路告警都可以视为环路类原因。

(5) 网络攻击类原因。常见的引起 CPU 占用率高的网络攻击包括 ARP 攻击、ARP-Miss 攻击、DHCP 攻击以及 TC BPDU 攻击等, 这些攻击行为的共同特点是攻击源产生大量的协议报文对交换机 CPU 进行冲击, 因此可以在交换机上看到大量的报文上送统计。判断 ARP 攻击和 ARP-Miss 攻击, 可以通过执行 `display arp packet statistics` 命令获取 ARP 报文统计信息, 重点关注 ARP Pkt Received 和 ARP-Miss Msg Received 统计信息, 根据其统计值的增长情况判断网络攻击类型。执行 `debugging arp packet` 命令打开 ARP 报文调试开关, 查看大量上送的 ARP 或 ARP-Miss 攻击源信息。判断 DHCP 攻击, 可以通过执行 `display dhcp statistics` 命令获取 DHCP 报文统计信息, 如果报文上送速度较快, 说明存在 DHCP 攻击。

(6) 配置错误类原因。由于网管同步操作或者用户命令大量输出信息到终端导致的, 该类情况的发生一般伴随着特定的网络管理事件, 配置错误会瞬间提高 CPU 占用率或造成交换机 CPU 短时间占用率升高, 如果暂停配置或取消配置命令发现 CPU 占用率降低则可配置错误原因。通过在用户模式下运行 `display cpu-usage` 命令可以采集 CPU 占用率高时各任务的 CPU 占用率, 当发现 AGNT 或 AGT6 任务 CPU 占用率过高时, 就可以确定 CPU 占用率高是网管同步等网管操作引起的, 当出现 VT 任务 CPU 占用率高时, 可以确定是用户命令大量输出信息到终端引起的。

3. 进行故障修复

针对故障原因不同需采用不同的故障修复方法。

(1) 硬件故障原因。判断故障根源可能为硬件故障时, 请先尝试手工复位 CPU 占用率较高的交换机, 去除交换机配置, 如果复位后问题依然存在, 可联系厂商进行处理。

(2) STP 震荡原因。如果是用户接口 Up/Down 引起的 STP 拓扑变化,则在接口视图下通过执行 `stp edged-port enable` 命令,将接入侧端口配置为边缘端口,并执行 `stp bpdu-protection` 命令开启 BPDU 保护功能。如果是发现根桥不断改变造成震荡时,则需要每台交换机执行 `stp root-protection` 命令开启根保护功能。

(3) 路由协议震荡原因。以 OSPF 路由协议为例, OSPF 邻居失连的主要原因有接口链路震荡、大量 LSA 泛洪报文等。当发生接口链路震荡时, 接口链

路震荡会导致 OSPF 邻居关系震荡, 可以通过日志信息查看接口 Up/Down 的记录情况, 请对接口链路进行检查。如果有大量 LSA 泛洪报文时, 会导致网络中产生大量的 LS UPDATE 消息, 此时交换机忙于处理 LS UPDATE, 可能会导致 Hello 报文得不到及时处理, 引起邻居状态 Down, 如果 OSPF 邻居超时时间配置小于 20s, 建议接口视图下通过 `ospf timer dead interval` 命令将 OSPF 邻居超时时间配置为 20s 以上。建议 OSPF 视图下通过 `sham-hello enable` 命令使能 `ospf sham-hello` 功能, 允许交换机通过 LSU 等非 hello 报文维持邻居关系。

(4) 网络环路故障。可以通过执行 `display cpu-usage [slave|slot slot-id]` 命令来确保是哪个子模块造成交换机 CPU 占用率高, 发现后可以利用接口指示灯的闪烁情况和通过执行 `display interface` 来确认各接口

流量情况, 如果仍方便排除时, 可在用户模式下执行 `loop-detect eth-loop alarm-only` 命令, 查看发生 MAC 地址漂移的接口, 也就是产生环路的接口, 还可以采用 1/2 法通过拔网线的方式来原因发生环路的接口, 排除环路故障或启动 STP/RSTP/MSTP 等生成树协议。

(5) 网络攻击故障。如果是 ARP 攻击、ARP-Miss 攻击和 DHCP 攻击, 可以通过开启自动攻击溯源功能的方式及时检测攻击行为, 如果网络中发生了攻击, 则在被攻击的端口通过 `stp tc-protection` 命令开启保护功能, 减少攻击对交换机的影响, 可以在找到攻击源后, 隔离接口或对攻击源进行故障排除。

(6) 配置故障。用户操作引起的 CPU 占用率高一般不会持续很长时间, 并且通常情况下不会影响业务, 如果造成业务故障且造成交换机 CPU 占用率高, 则为配置故障, 请清除该配置。

❖ 插错网线闹风暴

▼ 辽宁 冯志强 冯晓龙

某日, 单位很多部门反映上网质量不好, 打开网页很慢, 有时还打不开, 用飞秋在局域网内传几兆的文件都很困难。

故障分析

单位的网络拓扑结构是这样的, 由一台主交换机与上级相连, 不同楼层用光纤收发器连接到主机房的光纤收发池, 再与主交换机相连。同楼层采用交换机级联的方式为部门各终端提供接口。此次出现故障的部门分布较广, 几乎各楼层都出现了上网不好的现象。因为是全网性的问题, 于是把问题的焦点放在主交换机上。主交换机是华为 S5700 交换机, 观察各端口指示灯, 发现所有端口指示灯都在急速地闪烁。根据以往经验, 判断为交换机端口数据阻塞故障, 或因端口环路甚至网络蠕虫病毒造成的网络风暴。

排除步骤

首先排除交换机端口数据阻塞故障。先用一台终端 Ping 各楼层交换机, 出现严重的丢包现象。将主交换机断电重启。重启后, Ping 各楼层交换机的窗口显示正常。但好景不长, 不到 5 分钟, 部分楼层又出现丢包现象, 而且越来越多。最后所有窗口都出现了丢包严重的现象, 故障依旧。

进而确定因端口环路或网络蠕虫病毒造成了网络风暴。若要排除网络蠕虫病毒的可能, 需要对所有部门上百台终端进行病毒查杀, 时间太长, 所以决定先排除端口环路造成网络风暴的可能性。

用同一台终端持续 Ping 各楼层交换机。将主交换机通往各楼层的网线全部拔掉, 再逐一进行连接, 并观察各窗口丢包情况。当连接到五楼时, 开始出现丢包现象, 而且越来越严重。问题终于有了眉目!

五楼共有 4 台交换机级联使用, 机柜放在一个库房内。找来管理员, 问他有没有人动过机柜里的设备。

他说，上午会议室加了几台上网电脑，从这里接了两根网线，一根主用一根备份，并在会议室放置了一台交换机，连接各电脑。经过排查，确实有两根网线，从机柜上某个交换机的两个端口接到了会议室的交换机上，而且两根网线全插上了。问题原来在这里！虽然是末端的两台交换机出现了环路，却使整个局域网产生了风暴。将其中的一根网线拔掉，整个网络恢复正常。

经验总结

在实际工作中，造成网络连通质量下降的原因比

较多，如交换机端口阻塞、网络蠕虫病毒、端口环路，甚至网线质量差、强电干扰等。在判断故障原因时，要根据具体情况进行分析，结合网络拓扑结构，观察网络设备、询问变更细节，从易到难、从简到繁，逐步排除故障点。同时，在网络设备的管理上，也要指定有专业知识的人负责；在增减网络设备时，更要在专业人员指导下进行，并对增加的网络设备和线缆及时做好标签。否则，会出现牵一发而动全身的现象，影响全网正常运行。

语音业务单通故障分析

广东 黄国贤 叶世青

故障现象

阳江某个集团客户报障用户宽带业务正常，语音业务不稳定，出现通话几秒钟后无音或中断现象，通过 Ping 有语音问题用户的 ONU，出现间接性丢包。

故障分析

通过检查 OLT 配置，确认语音与宽带业务是走不同物理链路，语音业务走 gei_1/19/1 上行，宽带业务走 smartgroup1 聚合端口上行。查看语音网关设备告警及 OLT 日志、OLT 侧抓包分析如下：

1. 在 OLT 语音业务上联口 gei_1/19/1 数据包统计信息发现，Input 方向有严重丢包及 CRC 校验错误情况发现，OLT 语音业务上联口状态信息如图 1 所示。

```
ZX-OLT001-DongPingYouZhengGpon#show interface gei_1/19/1
gei_1/19/1 is up, line protocol is up
Input:
Packets      : 42506793   Bytes      : 6326660484
Unicasts     : 39971189   Multicasts : 0
Broadcasts   : 2506477   Undersize  : 25
Oversize     : 0         CRC-ERROR  : 29127
Dropped      : 42589     Fragments  : 13437
Jabber       : 0         MacRxErr   : 0
IncorrectVlanDrop: 26184
```

图 1 OLT 语音业务上联口状态信息

Input : ONU 回复信息方向，出现大量丢包，一般可能存在光路不好、接口协商模式不对、数据配置错误等问题。

通过排查，OLT 和 ONU 设备端口的收发光正常，双方端口是自动协商，并且通过更换两端对应接口的光模块，问题依旧。但是在排查过程中，发现有部分客户的语音在开通后一直能够正常使用，光路只有一条，只是 IP 地址属于不同网段，所以可能问题出在是数据配置上。

2. OLT 侧抓包分析

如图 2 所示，不正常丢包下的 ONU，从 OLT (10.102.234.1) Ping 问题 ONU (10.102.234.251) 时，ICMP Request 消息包在 SEQ=50/12800 之前都可以得到 ONU 的 Reply，但是在 SEQ=51/13056 之后，就没有收到 ONU 应答，直到 SN=414 广播消息发出后，才得到 ONU 的 Reply 消息。在此期间，有 6 个 ICMP Request 消息没有得到响应，中断时长约为 15 秒。根据 IP 通信原理，在局域网内是根据 MAC 地址来实际寻址的，此次问题应该为 ONU ARP 表项间歇性老化，未及时学习更新造成。

No.	Time	Source	Destination	Protocol	Length	Info
1	0.000000	10.102.234.1	10.101.234.1	ARP	60	Request for 10.101.234.1 (eth0)
2	0.000000	10.101.234.1	10.102.234.1	ARP	60	Response for 10.102.234.1 (eth0)
3	0.000000	10.102.234.1	10.101.234.1	ARP	60	Request for 10.101.234.1 (eth0)
4	0.000000	10.101.234.1	10.102.234.1	ARP	60	Response for 10.102.234.1 (eth0)
5	0.000000	10.102.234.1	10.101.234.1	ARP	60	Request for 10.101.234.1 (eth0)
6	0.000000	10.101.234.1	10.102.234.1	ARP	60	Response for 10.102.234.1 (eth0)
7	0.000000	10.102.234.1	10.101.234.1	ARP	60	Request for 10.101.234.1 (eth0)
8	0.000000	10.101.234.1	10.102.234.1	ARP	60	Response for 10.102.234.1 (eth0)
9	0.000000	10.102.234.1	10.101.234.1	ARP	60	Request for 10.101.234.1 (eth0)
10	0.000000	10.101.234.1	10.102.234.1	ARP	60	Response for 10.102.234.1 (eth0)

图 2 不正常丢包的 ONU

通过过滤出 ARP 广播包，发现有问题的 ONU 收到广播包的间隔时间约为 24 秒左右，序号为 445 和 583 之间间隔。而语音正常的 ONU 的广播报时间为 16 秒。

通过核查不正常 10.102.234.1 这个网段和正常的 10.101.234.1 这个网段的数据配置，发现正常网段的 IP，有一部分配到了其他 OLT 的用户，可能与此网段的 IP 分在不同的设备上有关，当其他 OLT 用户的 ARP 请求报文或是 ARP 广播报文是广播方式，又与这台 OLT 是同一个 VLAN，所以也会广播到这台 OLT 下，增大了频率。

至此问题定位基本可以判断出主要是由于 ARP 列表老化造成 ONU 没有 MAC 地址对应表，从而导致无法正常传送包，但是 ONU 基本没有什么配置内容，更换正常的 ONU 到有问题的网段，问题可以重现，所以推断出问题应该出现在 OLT 配置数据上。

3. 通过下载正常 OLT 的局数据配置和此台 OLT 配置进行比对，发现开局时为了满足集团客户 PON 口下不同用户语音业务互通需求，此台 OLT 开启了 MFF 代理功能（MFF：MAC Forced Forwarding，MAC 强制转发，可禁止同一子网的两个用户间直接互通，并把用户的上行流量强制转发到网关，由网关转发流量来实现用户间的三层互通），但 OLT 配置 MFF 代理 IP 所指向设备（OLT 上联 S9303 交换机）却未开启 ARP

PROXY 功能，导致此台 OLT 将所有用户语音 IP 的 ARP 请求转送到上层 S9303 时，此设备全未回复 ARP 请求，从而导致每隔一段时间即出现因终端不知网关 ARP 信息，而数据丢包情况发生。消息如图 3 所示。

解决方法

因为此台 OLT 下特殊组网，一个语音 VLAN 带 5 个 IP 网段，OLT 上设置 MFF 代理只能配置一个代理服务器 IP 地址，无法满足 5 个网段所有用户同 OLT 下互通需求，所以关闭 OLT 的此代理功能，在语音网关设备交换机上开启 ARP Proxy 功能，此 OLT 下不同用户二层互通，通过网关进行转发，即能防止广播泛洪，也能满足此语音 VLAN 下所有用户的互通问题。

维护建议

1. OLT 与上联设备对接时，建议两边端口模式配置一致，全部自协商或强制。
2. 语音业务 VLAN 下，建议一个 VLAN 一个 IP 网段，VLAN 下带用户越多，故障风险越高。
3. 建议 OLT 开启端口保护功能，能有效防止广播泛洪或用户电脑 ARP 病毒干扰其他用户业务等问题。
4. 当 OLT 下用户有互通需求时，建议由网关设备开启 ARP 代理功能。
5. 数据配置最好按照业务的标准模板进行，否则出现问题，需要耗费大量的时间进行排查，对于非标准模板配置时，一定要做好业务验证工作，防止业务开通后用户的投诉，提升用户使用感知。

修复 RedHat 虚拟机挂盘故障

贵州 郜荣杰

故障现象

近日笔者在某系统上线测试过程中，发现页面一直加载无法正常显示，并发现主机内存使用率高达 99%，

仅剩 100MB 内存可以使用。为保证资源尽早释放，决定重启（renboot）主机。重启后，发现原来附件数据盘没有自动挂载，通过手工挂载时出现如下错误：


```
[root@XXXXXX ~]# mount /dev/sdb5 /mnt
mount: wrong fs type, bad option, bad superblock
on /dev/sdb5,
missing codepage or helper program, or other error
In some cases useful info is found in syslog - try
dmesg | tail or so
使用 dmesg | tail 命令查看详细日志如下：
[sdb]Cache date unavailable
[sdb]Assuming drive cache:write through
[sdb]Attached SCSI disk
EXT3-fs error ( device sdb5 ):ext3_check_
descriptors:Block bitmap for group 640 not in group
(block 1340335608) !
EXT3-fs error ( sdb5 ):error:group descriptors
corrupted
```

故障处理

1. 首先为预防数据丢失，将挂载失败磁盘通过 VMware vSphere Client 进行备份，保证修复失败后数据丢失。

2. 备份成功后对备份磁盘进行恢复操作：
查看备份超级块的位置。

```
[root@XXXXXX ~]# mkfs -t ext3 -n /dev/sdb5
结果如下：
```

```
mke2fs 1.41.12 ( 17-May-2010 )
```

文件系统标签 =

操作系统：Linux

块大小 = 4096 (log=2)

分块大小 = 4096 (log=2)

Stride=0 blocks, Stripe width=0 blocks

32768000 inodes, 131070303 blocks

6553515 blocks (5.00%) reserved for the super user

第一个数据块 = 0

Maximum filesystem blocks=4294967296

4000 block groups

32768 blocks per group, 32768 fragments per group

8192 inodes per group

Superblock backups stored on blocks:

```
32768, 98304, 163840, 229376, 294912, 819200,
884736, 1605632, 2654208,
```

```
4096000, 7962624, 11239424, 20480000,
```

```
23887872, 71663616, 78675968,
```

```
102400000
```

修复坏数据块：

```
[root@XXXXXX ~]# fsck -t ext3 -b 163840 /dev/
sdb5
```

按块修复成功后，发现部分数据恢复，说明修复磁盘有希望，开始着手整盘修复。

```
[root@XXXXXX ~]# fsck -t ext3 /dev/sdb5
```

截止 3 个小时修复命令还没有完成，也没有任何进度条反映执行的进度。为更好地跟踪命令执行修复进度，使用“Ctrl+C”中断上述命令，使用如下指令：

```
[root@XXXXXX ~]# fsck -t ext3 -C -y /dev/sdb5
```

3. 历时 6 个小时完成数据恢复，恢复数据量为 270GB。

通过比对，恢复数据量与原来数字档建系统附件数据量大小相符。

4. 重新分配磁盘，通过命令 (scp -r /mnt root@主机 IP:/) 将恢复的数据导入到重新分配的磁盘中，启动应用服务后系统正常。

故障原因分析

文件系统损坏原因，一是非法关机，二个是磁盘有环道，只能一个一个排除，先软后硬，如果格式化后，还是有问题，那原因多半就是硬件的问题了。一般情况是由于非法关机引起的，重启主机时使用了 reboot 命令，此命令可以快速关闭系统，但如果还有其他用户（程序用户）在该系统上工作时，就会引起数据的丢失。使用 reboot 命令的场合主要是在单用户模式，其他模式建议使用 init 6, shutdown -r now, 防止因操作规范导致系统文件崩溃。

经验总结

1. 系统重启时应使用 shutdown -r now 命令，减少操作失误。

2. 加强系统文件备份管理，以防无法恢复造成损失。

3. 流媒体服务对系统内存占用高，应将其独立出来。

4. 应用系统主机应该设立定时重启机制，如 1 个月重启一下，在重启之前先做备份。

❖ 不可忽视电源线干扰

广西桂林 周瑜

故障现象

首先介绍一下简要的网络结构。因在陌生地域临时组建的网络，本级机房一台锐捷 RG-S2928G 交换机通过一对瑞斯康达 RC901-FE4E1 协议转换器，经光端机对开，远程接入上级三层网络交换机，通过普通六类网线下联一台普通交换机组成的局域网（在另外的工作间），带有十几台笔记本电脑终端，业务服务器放在机房，直接联接在锐捷交换机上，网关在上级。某天早上，因市电电压过低，不到 150V，于是通过一台 3KW、220V 的便携发电机对机房供电。进行系统测试时，发现终端不能登录服务器，而且通过 Ping 测试服务器，网络断断续续，丢包率超过 50%。Ping 网关，网络现象也是一样。

故障排查

出现故障，一般采用分段法，按照先内后外来排查。首先检查内部网络的问题。断开上联的网线，在终端上 Ping 服务器 IP 地址，现象一样。于是断开机房下联的网线，终端间相互 Ping 测试，没有丢包现象，网络正常，故障应该在机房。

在机房的锐捷交换机上直接连一台笔记本终端，并且 Ping 服务器 IP 地址，也出现严重丢包。因只是 1 台交换机下带一台服务器和一台终端，问题应该在交换机上，怀疑是交换机出了故障。直接换上备用的交换机，但故障依旧。

此时，有点迷糊了，用市电时好好的，服务器是新用的，说明设备应该是没有问题。听着旁边发电机的噪音，想起了是不是电源线的干扰呢？因为只知道强弱电线布线时不能走同一个线槽，并且要间隔一定的距离，如果有干扰，症状也没有见过。于是查双绞线和从发电机拉过来的主电源线，看是否有交叉或靠得很近。因为是由他人搭建的临时机房，线路布置有

点凌乱，好在线路并不多，容易理清线路走向，果然发现从发电机来的电源线和往工作间的六类双绞线基本靠在一起。毫不犹豫地按照强电与弱电路路分开走，并隔开足够的距离，特别是主电源线缆，单独从一个地方引进。整理完后，再测试网络，一切恢复正常。

故障分析

对于结构简单的网络，直接采取分段排查方法，逐步缩小范围。针对此类故障，在网上再次学习了一下相关强弱电综合布线知识，按综合布线规定：网线与电源线不能在同一方向并列。如果必须走，要用不同的线槽，距离 20cm ~ 50cm，最好不交叉。实际上，任何功率不超过 13W 的设备都可以从 RJ45 插座获取相应的电力，如 PoE(Power Over Ethernet)供电。因此，电脑终端的电源线对网线的影响是很小的。同时也进一步查明了双绞线与电力电缆的分隔距离，以及干扰源要求的分隔距离（如表 1 和表 2 所示）。

表 1 电力电缆分隔表

电缆类型	电力电缆与用户电缆分隔距离	
	并行	交叉
超低电压(AC<42.4V DC<60V)	无特殊要求	无特殊要求
低电压 (AC<1000V DC<1500V)	无间隔 50mm、有 间隔 25mm	间隔物厚度 6mm， 间距 25mm

表 2 电气噪音分隔表

干扰源功率 (KVA)	电力电缆与通信电缆间隔距离	
	非屏蔽通信电缆	屏蔽通信电缆
功率 <1KVA	300mm	25mm
1KVA< 功率 <2KVA	450mm	50mm
2KVA< 功率 <5KVA	600mm	150mm
功率 >5KVA	1500mm	300mm

从以上要求的分隔距离来看，这次故障的出现可以看成是大功率电源的干扰，与实际情况是相符的。通常所用市电为 220V，一般需要 5A ~ 10A 电流，对网线有影响，在强电流环境下产生的电磁波对网线的传输信号有影响，对信号的质量有影响。

经验总结

1. 在平时的网络维护中, 布线是首要解决的问题, 保证强弱电必须按要求分开。即使是临时搭建网络, 也要按要求执行, 以免存在干扰隐患。这次故障所幸的是网络结构很简单, 断几次线即可定位故障点, 否

则不知会走多少弯路。

2. 若仅针对网络丢包故障, 还应当考虑病毒、协商模式物理链路等可能。在熟悉网络结构的情况下, 执行分段排查, 逐步缩小故障范围, 可以少走很多弯路, 这也是网络管理员的基本处理方法。

路由器 IOS 灾难恢复

福建 李进珍 马记

路由器 IOS 相关概念

1. 路由器硬件组成

路由器主要作用是路由选择, 同时实现广播域隔离、异构网络数据包转发等功能。其硬件组成类似于一台特殊用途的计算机, 路由器硬件包括 CPU、内存、BOOT ROM、NVRAM、Flash 和各种各样的物理接口。

2. 路由器的引导过程

Cisco 路由器开机, 首先执行一个开机自检过程, 诊断验证 CPU、内存及各个端口是否正常, 紧接着路由器将进入初始化。

(1) 执行 ROM 中的引导程序加载, 它和计算机中的 BIOS 很类似, Bootstrap 会把 IOS 装到 RAM 中。

(2) IOS 可以存放在许多地方 (Flash、TFTP 服务器上或 ROM 中), 路由器寻找 IOS 映像的顺序决于配置寄存器的启动域以及其他的设置。

(3) 路由器开机检查配置寄存器, 判断执行 ROM 监控程序或 IOS 子集, 还是引导 IOS。装载 IOS 时, 会提示解压缩 IOS (这时出现许多 #), 如此时按下组合键, 装载和引导 IOS 的过程就被终止, 会进入 ROM 监控程序状态。否则, 引导完 IOS 后, 就把控制权交给 IOS。IOS 读取配置寄存器值, 判断是忽略现有的配置文件 (0x2142), 还是使用现有的配置文件 (0x2102)。

路由器 IOS 灾难恢复

不同类型的思科路由器, IOS 恢复的方式也有所不

同, 基本上可分为前期和后期两个版本, 前期主要针对低端路由器, 后期针对中高端路由器, 下面分两个内容进行说明。

1. 通用 Cisco 4000 以下系列恢复方法

(1) IOS 映像恢复步骤

连接 PC 的 COM1 口与路由器的 Console 口, 使用 PC 的超级终端软件访问该路由器。开启路由器的电源开关, 并在 30 秒内按下键盘的 Ctrl+Break, 中断路由器的正常启动, 进入 ROM 监视模式。因为该系列路由器不允许在正常工作状态下重写 flash memory, 所以只有进入 ROM (或 bootflash) 启动模式才能恢复 IOS 映像, 键入如下命令:

```
>o /r 0x2101 // 改变路由器虚拟寄存器的默认值 (0x2102)
```

键入重启命令:

```
>i
```

路由器重启后, 当屏幕显示以下信息, 表明路由器重启完毕, 路由器在虚拟寄存器的值为 0x2101 时自动进入 ROM 启动模式:

```
router (boot) >
```

此时, 将 TFTP 服务器上的 IOS 映像文件恢复至路由器 flash memory 中, 依次键入以下命令:

```
router (boot) >en
```

```
router (boot) #copy tftp flash
```

最后显示 Loading igs-i-l.110-22a.bin from 192.168.18.168 (via Ethernet0) : !!!!!!!!!!!!!!! (! 表示恢复成功)。

还原路由器虚拟寄存器的默认值 (0x2102), 恢复路由器的正常启动顺序。

```
router (boot) #conf t
router (boot) (config) #config-register 0x2102
router (boot) #reload
```

(2) IOS 映像升级方法

升级之前先备份, 将相关文件备份至 TFTP 服务器, 键入如下命令:

```
router#copy bootflash tftp (Cisco 2500 系列路由器不存在 bootflash, 相应的是 ROM)
```

```
router#copy flash tftp
```

```
router#copy startup-config tftp
```

以下操作与恢复方法步骤一致。

2. 通用 Cisco 7000 以上 (含 3600) 系列恢复方法

(1) IOS 映像恢复的方法

方法一: 使用 Xmodem 命令进行恢复

连接电脑的 COM1 口与路由器的 Console 口, 使用电脑的超级终端软件访问该路由器。开启路由器的电源开关, 并在 30 秒内按下键盘的 Ctrl+Break, 中断路由器的正常启动, 以进入 ROM 监视模式。

键入 xmodem 命令:

```
rommon 1>xmodem c3640-i-mz.120-10.bin (IOS 映像文件名)
```

路由器等待从 PC 上接收该 IOS 映像文件, 此时在超级终端点击发送选项, 选择存放在 PC 本地硬盘中的 IOS 映像文件, 确定后即开始下载文件至路由器的 Flash 中。由于通讯带宽只有 9600 波特, 整个文件下载时间约为 1.5 小时 (依文件大小而定)。

接着, 路由器将自动重启, 恢复完毕。

方法二: 使用 tftpdnld 命令进行恢复

进入监控模式, 将路由器的 eth0/0 口 IP 地址设为 192.168.1.22/24, PC 机 IP 地址设为 192.168.1.23/24。将要升级的 IOS 映像文件拷贝到相关的目录中, 并运行 TFTP 服务器软件, 设置拷贝 IOS 映象文件目录。

通过 set 命令查看配置参数, 执行 tftpdnld 命令进行 IOS 恢复:

```
rommon 5>tftpdnld
```

执行 tftpdnld 命令进行 IOS 升级, 有时可能会报错或命令不执行, 这时只要用 sync 命令保存配置后, 重新启动路由器 (最好关掉电源再开机) 后, 再执行 tftpdnld 命令。

系统重启: 在 rommon 13 > 提示符下键入 reset, 或重新启动路由器, 进入正常的引导状态。

(2) IOS 映像升级的方法

同理, 升级之前先备份, 将关键文件备份至 TFTP 服务器, 键入下列命令:

```
router#copy bootflash tftp (Cisco 3600 系列路由器不存在 bootflash)
```

```
router#copy flash tftp
```

```
router#copy startup-config tftp
```

因为 Cisco 7000 系列路由器允许在正常工作状态下重写 Flash, 所以直接键入以下命令, 就可以完成 IOS 映像的在线升级:

```
router#copy tftp flash
```

```
router#reload
```

3. 思科定义 IOS 恢复方法

思科发布的 ID 15082 文档, 针对 7000 系列路由器设备提出不同情况时应采取的灾难恢复方法, 其操作程序归纳起来主要包括四种措施, 一是检查路由器引导配置寄存器启动域是否正确, 造成路由器无法正常引导, 如果错误则更改寄存器数值进行恢复。二是查找定位系统存储位置, 确定有效的 Flash 存储器, 指定引导位置进行恢复系统。三是使用 TFTP 服务软件下载有效的引导系统。四是使用别的兼容路由器进行 PCMCIA 卡系统复制实现恢复。

(1) 寄存器配置错误时恢复

当路由器每次开机引导时都自动进入 ROM 监控模式, 排除故障要先检查配置寄存器启动域数值是否正确, 7000 系列路由器配置寄存器第四位为引导表示, 如果此值为 0, 路由器使用默认 IOS, 即引导时配置寄存器数值后四位为 XXX0 ???, 系统将会进入 ROM 监控模式, 只能通过手动输入命令的方式操作, 输入 confreg 命令来修改引导:

```
rommon 2 > confreg // 回车
```

```
console baud: 9600
```

```
boot: the ROM Monitor
```

```
do you wish to change the configuration? y/n [n]:
```

上述表明寄存器指示路由器上电使用 ROM 监控模式引导方式, 如果要使用默认的思科 IOS 引导, 需要改变寄存器数值, 具体操作如下:

```
change the boot characteristics? y/n [n]: y
```

```
enter to boot:
```

```
0 = ROM Monitor
```


1 = the boot helper image

2?15 = boot system

[2]: 2

boot: image specified by the boot system commands
or default to: cisco2?C7200

路由器应恢复正常引导。

(2) 查找有效引导镜像的 Flash

如果寄存器数值设置正确,并且在引导开始时没有中断路由器启动,一般来说路由器应该能够正常引导。可如果路由器引导仍然自动进入 ROM 监控模式,主要原因可能是路由器找不到有效的引导镜像。这种情况下,首先要在路由器存储单元中查找有效的引导镜像,使用 DEV 命令进行查看:

```
rommon 1 > dev
```

```
bootflash: boot flash
```

```
slot0: PCMCIA slot 0
```

```
slot1: PCMCIA slot 1
```

```
eprom: EPROM
```

接下来输入 dir [device ID] 命令,在每个存储单元查找有效的引导镜像(ID为 slot0/1 是对应的 PCMCIA 卡的位置),如果提示是“坏的系统名称”,表示系统设备可能是无法读取。

```
rommon 2 > dir slot0:
```

```
File size Checksum File name
```

```
12566060 bytes (0xbfbe2c) 0x38d1c81b c7200-  
ik8s-mz.122-10b.bin
```

如上提示,在 slot0 中有可用的引导镜像,使用 boot 命令进行引导。

```
rommon 3> boot slot0:c7200-ik8s-mz.122-10b.bin
```

路由器现在能够正常引导。但有时出现所有存储单元都没有有效的引导镜像,致使引导失败,其原因一是所有存储单元是空的(提示“No files in directory”)。二是存储单元使用路由器无法识别文件系统格式(提示“device does not contain a valid magic number”)。三是设备不能正常工作(提示“trouble reading device magic number”)。四是 IOS 软件是损坏的。

遇到上面这种情况,必须使用 TFTP 或者其他路由器的 PCMCIA 卡下载引导系统。

(3) 从 TFTP 服务器下载系统

操作方法可参考前面 IOS 映像恢复的方法及步骤。如果主镜像和引导镜像文件都被删除了,那么只能通过交换 PCMCIA 卡来进行恢复。

(4) 交换其他路由器 PCMCIA 卡获取系统

首先要找到一台相同的路由器,或具有兼容 PCMCIA 卡的路由器,用以使用 Flash 卡恢复路由器。如果两台路由器同一系列的,可以直接使用好的 Flash 卡引导待恢复路由器,由于路由器使用 RAM 运行系统,使用 TFTP 或者直接读取 RAM,在热插拔 PCMCIA 卡情况下进行引导系统拷贝。如果两台路由器不同,但使用的 PCMCIA 卡兼容,可使用另一台正常引导的路由器将引导镜像发送到 Flash 卡。

以上四种方法或条件都不具备,只能把路由器发给厂家进行处理。

路由器 IOS 故障处置案例

案例一:一台 Cisco 3640 路由器进行 IOS 升级时,由于误操作不慎关闭电源,路由器无法正常启动。启动后到 rommon 1 > 状态。

处理方法:

先分析故障出现的可能点位,根据了解的情况确定是路由器升级失败,IOS 缺失导致无法正常启动,自动进入了监控模式。

第二步,准备恢复的工具软件及系统,首先通过 show version 命令,确定 RAM 与 Flash 闪存大小,从思科官网下载当前可以安装的 IOS 版本。GD(常规部署版本,属于最稳定的版本)、ED(早期开发版本,意味着会存在较多的 bug)、LD(限制版)、DF(延期版),推荐使用 GD 版本。使用 PC 机安装 TFTP 服务软件,并拷贝 IOS 系统到下载目录。

第三步,连接路由器 Console 口,按照“通用 Cisco 7000 以上(含 3600)系列 恢复方法”中方法二描述的步骤进行恢复。最后,重启路由器后故障消除。

注意

路由器系统升级时,一定要进行系统备份,将原有系统备份到终端上。如果路由器 Flash 空间较大,也可以重命名到本地,防止升级失败能尽快恢复。进行升级操作时,尽可能使用 UPS 供电,保证电源稳定,避免因断电损坏系统。

案例二:单位使用一台 Cisco 7200 系列路由器,外出保障时因删除配置文件失误。将 IOS 文件删除后进行了格式化处理,致使路由器无法进入引导系统。

处理方法：

根据以上方法进行处理，发现无论使用串口 Xmodem 还是 TFTP 服务器方式进行恢复，都不能恢复系统，主要原因是该设备在监控模式下不支持 Xmodem 文件传输，使用 TFTP 进行到 tftpdnld 上传文件时系统报错，同步保存没有效果，多次尝试都无法恢复。

查阅官网相关资料，决定采用“交换其他路由器 PCMCIA 卡获取系统”方式恢复系统。找到一台同型号的路由器，利用其 PCMCIA 卡正常引导故障路由器，将卡存储的内 IOS 拷贝到 PC 终端，而后插入已被格

式化的卡（此时路由器因系统读入 RAM，仍正常运行），在线通过 TFTP 将备份的 IOS 拷贝到卡内，重启路由器后恢复正常，但引导速度偏慢，分析可能原系统版本较低，下载新版本升级后运行正常。

注意

特别情况下，要采取多种应急恢复方法，区别不同类型设备，选择适当地恢复方法。由于路由器 ISO 版本较多，选择时要慎重，一般采取先恢复再升级的程序，保证路由器“使用最新、最可用的版本”。

交换机端口不可用解析

湖北 程东亮

故障现象

电脑无法上网，连接该电脑的交换机（Cisco 2950，Version 12.1（6）EA2a，RELEASE SOFTWARE（fc1））端口物理指示灯灭或者显示为橙色（不同平台指示灯状态不同）。使用 show interfaces 命令显示该端口状态如下：

FastEthernet0/22 is down, line protocol is down (err-disabled)。

查看系统日志信息，显示如图 1 所示。

```
•Mar 15 15:47:19.984: %SPANTREE-2-BLOCK_BPDUGUARD: Received
BPDU on port FastEthernet0/22 with BPDU Guard enabled.
Disabling port.
•Mar 15 15:47:19.984: %PM-4-ERR_DISABLE: bpduguard error
detected on Fa0/22, putting Fa0/22 in err-disable state.
•Mar 15 15:47:21.996: %LINK-3-UPDOWN: Interface
FastEthernet0/22, changed state to down.
```

图 1 日志信息

故障原因

交换机端口处于 err-disable（错误不可用状态）的原因可以使用 show errdisable detect 命令来查看，显示

如图 2 所示。

ErrDisable Reason	Detection status
Uddid	Enabled
bpduguard	Enabled
security-violatio	Enabled
channel-misconfig	Enabled
link-flap	Enabled
loopback	Enabled

图 2 交换机端口故障原因查询

以上列出了交换机端口被置为 err-disable 的所有原因，具体是什么原因导致当前端口状态为 err-disable，则可以使用 show interfaces status err-disable 命令来查看，显示如下：

```
Port Name Status Reason
Fa0/22 err-disabled bpduguard
```

可以看出，是由于 bpduguard（BPDU 防护）的原因导致当前端口状态变为 err-disable。

故障解决方法

在缺省配置下，一旦端口被置为 err-disable，IOS

将不会试图恢复该端口，只能通过手动配置 `errdisable recovery cause` 命令来重新激活 `errdisable` 的端口。本故障可以使用 `errdisable recovery cause Bpduguard` 命令来使该端口恢复到正常状态，但是，如果引起 `errdisable` 的源没有根治，在恢复正常状态（缺省时间为 300 秒）后，端口会再次被置为 `err-disable`。

下面对导致交换机端口处于 `err-disable` 状态的几个常见原因进行详细分析，并给出解决方法。

1. 通道配置错误

第一个原因是通道配置错误。当 FEC 两端配置不匹配的时候，就会出现 `err-disable`，假设 Switch A 把 FEC 模式配置为 `on`，这时 Switch A 是不会发送 PAgP 包与相连的 Switch B 去协商 FEC 的，它假设 Switch B 已经配置好 FEC 了。但事实上 Switch B 并没有配置 FEC，当 Switch B 的这个状态超过 1 分钟后，Switch A 的 STP 就认为有环路出现，因此也就出现了 `err-disable`。

解决办法：

把 FEC 的模式配置改为 `channel-group 1 mode desirable non-silent`，即只有当双方的 FEC 协商成功后，才建立 channel，否则端口还处于正常状态。

2. 双工不匹配

第二个原因是双工不匹配。一端配置为 `Half-Duplex` 后，它会检测对端是否在传输数据，只有对端停止传输数据，它才会发送类似于 ACK 的包来让链路 Up，但对端却配置成了 `Full-Duplex`，它才不管链路是否是空闲的，它只会不停地发送让链路 Up 的请求，这样下去，链路状态就变成 `err-disable` 了。

解决办法：

两端端口双工模式配置一致即可。

3. BPDU 端口防护

第三个原因 BPDU 端口防护，也就是与 `portfast` 和 `BPDU guard` 有关。如果一个端口配置成了 `portfast`，也就是说该端口应该和一个电脑相连，该电脑是不会发送 `spanning-tree` 的 BPDU 帧的，而网络管理员同时不小心在该端口上配置了 `BPDU guard` 来防止未知的 BPDU 帧，以增强安全性，于是该端口接到了 BPDU 帧，这个端口自然就进入到 `err-disable` 状态了。

解决办法：

取消端口 `bpdu` 防护或者直接把端口 `portfast` 功能关掉。

4. 单向链路检测

第四个原因是单向链路检测。单向链路检测（UDLD）是 Cisco 的私有二层协议，用于检测链路的单向问题，有的时候物理层是 Up 的，但链路层是 Down 的，这时候就需要 UDLD 去检测链路是否是真的 Up 的。当 AB 两端都配置好 UDLD 后，A 给 B 发送一个包含自己 Port ID 的 UDLD 帧，B 收到后会返回一个 UDLD 帧，并在其中包含了收到的 A 的 Port ID，当 A 接收到这个帧并发现自己的 Port ID 也在其中后，认为这链路是好的。反之就变成 `err-disable` 状态了。

假设 A 配置了 UDLD，而 B 没有配置 UDLD，A 给 B 发送一个包含自己 Port ID 的帧，B 收到后并不知道这个帧是什么，也就不会返回一个包含 A 的 Port ID 的 UDLD 帧，那么这时候 A 就认为这条链路是一个单向链路，自然也就变成 `err-disable` 状态了。

解决方法：

使用命令 `udld reset` 来重启所有被 UDLD 关闭的接口。

5. 链路抖动

第五个原因就是链路的抖动。诸如网线问题、速率不匹配、双工不匹配或者千兆 GBIC 卡故障等原因，使该链路在 10 秒内反复 Up、Down 五次，那么就进入 `err-disable` 状态。

解决方法：

换一根好网线或两端端口速率、双工模式配置一致或更换端口即可。

6. 环路

第六个原因就是 `keepalive` 环路。在 12.1EA 之前，默认情况下交换机会在所有的端口都发送 `keepalive` 信息，由于不同的交换机之间协商 `spanning-tree` 可能会有问题，一个端口又收到了自己发出的 `keepalive`，那么这个端口就会变成 `err-disable` 了。

解决办法：

把 `keepalive` 关了，或者把 IOS 升到 12.2SE。

7. 端口安全惩罚

最后一个原因是端口安全惩罚机制，相对简单，就是由于配置了 `port-security violation shutdown`。

解决方法：

重新使用 `no shutdown` 命令开启该端口。

❖ 广告代码为何无法解析

广东 赖文书

故障现象

一天，有用户反馈访问 FPO（www.freepatentsonline.com）很慢，而笔者在自己电脑上测试访问很正常。freepatentsonline 是一个专利查询网站，提供专利申请专利查询与下载，而笔者手边没有可查询的内容，无法进一步测试。

通过 VNC 远程连到用户 A 那边查看，检索查询一条数据要等 1 分钟左右的时间才能返回结果，再打开结果集中条目的具体内容页面也很慢。将查询的专利号在笔者的电脑上操作很快就返回了结果，访问具体内容页面也很正常，用户说 FPO 这么慢的问题是最近一周左右出现的，以前一直很好。

故障诊断

由于这些用户经常访问国外网站，部分网站受限无法访问，公司为其提供了一条专线，这些计算机的 IP 路由是从防火墙上的专线接入互联网的，专线结构如图 1 所示，公司出口网络拓扑如图 2 所示。笔者因前些时间测试的需要，也将自己的计算机 IP 路由调到了专线 x3 出口，也就是和他们出口一样，访问同样的网站在检索速度上却差别很大。

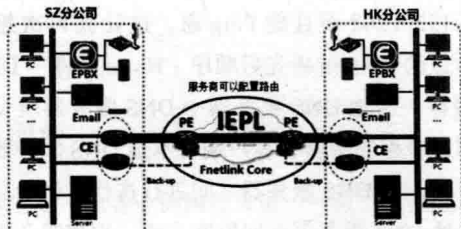


图 1 专线拓扑结构

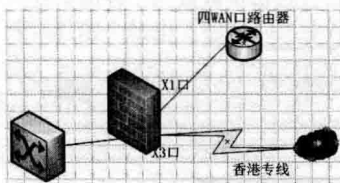


图 2 公司出口网络拓扑

首先从上网行为设备上将自己调入他们的用户组，这样两者所应用的上网行为管理策略也一样了，但是笔者计算机的检索速度也是很快的。难道用户浏览器有问题？但是用户以前访问一直没问题，而且浏览其他网页没有很慢的现象，故此种可能排除。联系专线服务工程师，因该网站禁 Ping，通过 tracert 检测到 FPO 网站的速度和路径也是正常的。

第二天远程连到用户 B 继续研究，我们的计算机都是使用的 IE8，用户另外还装有 Chrome 浏览器，其访问 FPO 也是一样的检索很慢，好像比 IE 略快一些。难道是上网行为管理设备对此检索的返回结果有影响？将该网址查询的到 IP 加入全局排除，同时将用户 IP 开启直通，在检索返回结果集时好像快了一些，但是访问具体内容页面仍然是很慢。

无助的情况下又咨询了深信服 AC 上网行为管理工程师，通过 Chrome 浏览器的“开发人员工具”的 Network 项显示，FPO 检索返回结果慢就是卡在一条 HTML 脚本失败（如图 3 所示），该脚本等待服务器响应最后 Failed to load response data 占用了差不多 30 秒。

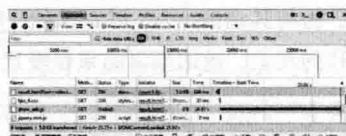


图 3 具体内容页脚本加载失败

我们知道浏览器是按顺序来读取网页中的代码，当输入专利号开始 Search 网页很快显示了总数信息，迟迟不见返回检索结果集，浏览器状态栏的进度条很艰难地

移动，这可能就是长时间处于等待状态的直接原因。可是笔者访问 FPO 的速度却很正常，这又是为什么呢？请求小组同事支援，测试 FPO 检索返回结果也很正常。再多次观察用户 A 和 B 打开 FPO 详细内容页面和本机打开时的情况，发现他们的页面居然没有广告，而笔者这边先是出现广告，紧接着很快出现检索的详细数据内容（如图 4 所示）。此广告正是前面所看到的 HTML 脚本 show_ad.js 加载的，在笔者的计算机几毫秒就完成了，所以整个检索过程很快就返回了查询信息。

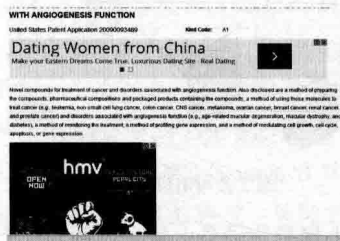


图 4 带广告的详细内容页

全方位排查

第三天远程检查用户 C 的情况和上面一样，打开首页很正常，任意检索一个数据返回结果集就开始慢起来，同样是没有广告。也就是说访问 FPO 慢是因为广告被拦截导致的。从网络方面考虑，防火墙上是一样的出口，也是同样的 NAT 策略，只是我和他们所属不同网段 VLAN207 和 216，前者的网关在防火墙前面的核心交换机，后者的网关在另一大楼汇聚层交换机，所以 tracert 显示本机机会比他们的少一跳。通过将本机所接交换机端口改为 VLAN216 测试访问 FPO 依然正常。软件方面能想到的可能有深信服上网准入插件和防病毒软件影响。

拿笔记本电脑去用户那里测试，先试试这边访问 FPO 的速度怎么样，通过多次检索发现有时快有时慢，VLAN207 默认走的防火墙 X1 口四 WAN 口路由器接入互联网的，再将其调到走 X3 口专线时，笔记本出现了和用户一样的现象，返回检索结果很慢且无广告。

重点突破

立刻安装了 360 安全浏览器，并使用其浏览器医生进行修复，结果也一样的令人沮丧。关闭防病毒软件和卸载深信服上网准入插件，也不见任何起色。详

细对比了台式机和笔记本电脑，均是 64 位的 Windows 7 SP1 旗舰版，通过 systeminfo 命令对比其补丁也相差无几，台式机多了一个远程服务器管理工具相关的 KB958830。再仔细查看“开发者工具”Network 项中无法加载的脚本信息，Request URL: http://pagead2.googlesyndication.com/pagead/show_ads.js，和广告信息（如图 5 所示），这广告显示应该和 Google 有关。



图 5 Web 页中广告的信息

搜索“Google 广告不显示或者拖慢网页加载”，找到一条“如何解决百度广告不显示拖慢网页或打不开”Web 页，和自己遇到的故障现象极其相似，只是广告商不同。文章中作者因为更换宽带服务商后，出现了凡是带有百度广告代码的网面总是打不开或者极慢，亦或是勉强打开了也不显示广告。作者怀疑是新的宽带商默认的 DNS 服务器屏蔽了百度广告所致，并通过修改他的笔记本 DNS 完美解决了问题。可是我的笔记本和台式机均是局域网内 DHCP 服务器自动分配的，DNS 也是完全一样的。虽然没有直接解决我的问题，但是把我引向了解决问题的正确思路，不再纠结内部网络或者客户端方面的影响。

广告不显示并不是被拦截，而是未能正确解析相关域名地址，顺着这个思路突然想起了自己的台式机，曾经从网上下载并替换访问 Google 的 Hosts 文件，立即测试替换前后 Ping pagead2.googlesyndication.com 结果（如图 6 所示），不使用网上 Hosts 文件前的域名解析成了 203.208.41.153 并且不通，使用后解析成了 203.133.8.242 而且能 Ping 通，这让我再次想起了以前学过的 DNS 解析先后顺序：Hosts 文件→DNS 解析器缓存→本地 DNS 服务器→DNS 服务器所设置的转发器或者根服务器，客户端与本地 DNS 服务器进行递归查询，而 DNS 服务器之间进行迭代查询最后将结果由本地 DNS 服务器返回给客户机。困惑我几天的问题终于找到答案，还是专线对于本地非权威应答解析 pagead2.googlesyndication.com 的地址不通，导致广告无法加载拖慢了 FPO 检索结果返回的速度。最后联系专线服务商调试路由，让用户检索 FPO 恢复了正常。



图 6 替换 Hosts 文件 Ping 的结果不同

笔记本检索 FPO 的速度有时快有时慢，还有同事电脑在测试访问 FPO 为什么又是正常的呢？深入测试发现 4WAN 口的路由器接入互联网中，有 2 口能正常 Ping 通 pagead2.google syndication.com，此时通过 IE8 访问 http://pagead2.google syndication.com/pagead/show_ads.js 在浏览器就有下载文件窗口弹出，如图 7 所示，在另外 2 口无法 Ping 通时就没有任何反应，而路由器智能负载均衡模式为连机数均衡使得客户端获得的出口在动态变化中，所以出现笔记本从普通线路访问 FPO 有时快有时慢，当调到专线时就很慢的奇怪现象。

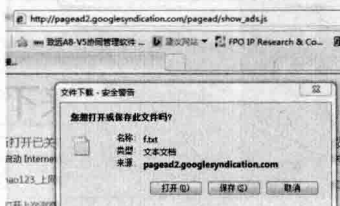


图 7 能 Ping 通时打开链接有下载提示

经验总结

整个问题处理过程由于经验不足，未能及时抓住重点突破，只能全方位地排查，占用了很长时间。防火墙 X1 出口网络的不确定性，又为故障排查增加了难度，特别是自己的计算机 Hosts 文件被修改给排查带来了莫名的困惑，如果 Hosts 文件未修改，就能很快确认是专线的问题，只是在联系专线服务商居然未能及时找到具体的原因，或许他们只是关心专线的链路速度和路由，在具体应用上超出了他们的作业范围。

所以，首先要自身专业知识经验过硬，才能和相关的服务商有效协调及时解决问题。处理 IT 问题需要先界定范围，逐步分层排除可能的问题点，再复杂的故障现象最后都能从基本原理中反推出其具体原因。

摆脱强制升级

山东 周宁

故障现象

笔者是一家企业的网管人员，一天，有位同事说她的电脑提示“重启电脑以完成 Windows 10 安装”（笔者单位是一家软件研发公司，标配的操作系统都是“Windows 7”，如果贸然升级到 Windows 10，会给工作带来诸多不便）。来到现场一看，发现此提示是一个叫“Windows 10 易升 V1.2”（以下简称“易升”）的程序窗口。

故障分析

这个软件在“程序和功能”以及“查看已安装的更新”中都没有它的身影。同事说，她自己并没有安装过 Windows 10 升级工具之类的软件，从而判断可能是微软推送过来的。笔者也没有遇到过此类的问题，只好告诉同事，先不要重启。

查找相关资料，发现“Windows 10 易升 v1.2”是一

款微软官方应用,可以使用 360 软件管家卸载,但试了一下,软件管家并不能发现这个软件,所以无法完成卸载。没办法,只好自己来做测试了。

测试的方法就是找一台虚拟机(我用的是 VMware 虚拟桌面)来模拟这个“事件”,还好笔者经常做些小测试,有现成的 Windows 7 虚拟机。先做好快照(之所以选择虚拟机,就是因为它可以无限地打快照,一个不行可以短时间恢复再试下一个),下载了一个“Windows 10 易升 v1.2”,并主动安装,安装完成后开始自动下载升级文件,经确认后发起升级,到最后弹出如图 1 所示界面。系统重启后就开始了 Windows 10 的安装过程。



图 1 Windows 10 升级提醒界面

故障解决

经过一番测试,终于找到了“完美”的解决方法。测试过程就不多说了,下面就给大家介绍一下详细的解决过程。

首先请用户把 C 盘的文件备份到其他硬盘,做好最坏的打算。

1. 在系统电脑重启之前,按下“Ctrl+Alt+Del”打开任务管理器。

2. 选择“进程选项”,找到“Windows10 Update”,并结束这个进程,如果报其他的错误,一概“确定”即可。如果您和我一样是主动安装的,需要打开“应用程序”选项,并选中“Windows 易升 v1.2”,点击“结束任务”,结束易升,重启也不会发生。

3. 打开“msconfig”,在“系统配置”界面的“引导”页,选中如图 2 所示的“(\windows)”(实验证明此项即为 Windows 10 的升级项),选择“删除”(如图 2 所示)。删除完成后,单击“确定”按钮。

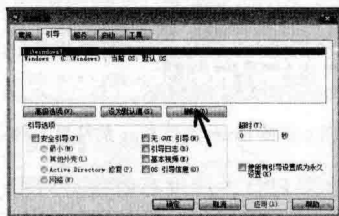


图 2“系统配置”界面

4. 在接下来出现的界面中,选择“退出而不重新启动”(因为我们还需要完成卸载易升)。

5. 下载“完美卸载(试用版就可以)”并安装,打开“完美卸载→卸载软件”页,注意图 3 所示页面左下角划线部分:此时即可按提示,将“Windows 10 易升 v1.2”图标拖入回收站。也可以将桌面的图标直接拖到“软件垃圾箱”中(推荐方式)。等扫描完成后,点击“开始卸载”。



图 3 完美卸载界面

6. 完成卸载后,重启系统,心爱的 Windows 7 又回来了。然后又叮嘱同事,关闭系统自动升级,以及安装 360 卫士,避免再次中招。

注意

文中所涉及软件均为免费版或者试用版,且已在解决问题后删除。



用交换机监测网络环路

福建 李贵华 马记 黄荣青

故障现象

笔者单位的内部局域网是典型的三层交换网络，核心交换机采用的是 H3C S7503 三层交换机，架设在单位网管机房，其中共划分 13 个 VLAN。分公司和三个办事处的汇聚交换机通过 VPN 方式接入核心交换机。公司总部的各业务部门通过超五类线或者光纤接入相应的汇聚交换机。某天财务部门电话报告办公网丢包严重，不能正常连接 ERP 系统和 OA 系统，检查网络发现网络延时很大，数据传输不稳定，请求帮助解决。一个小时后生产车间和人力资源办公室陆续报告相类似的故障。

故障定位

接到故障报告后，笔者通过查阅相关资料发现这些故障位置同属 VLAN6，即 VLAN6 的网络存在丢包严重的问题。其他 VLAN 数据收发正常，数据包延时小于 1ms，且无丢包。由此确定故障范围仅限 VLAN6。由于 VLAN 可以抑制广播风暴，不影响网内其他 VLAN，因此怀疑 VLAN6 内存在广播数据，过多占用网络资源，不能保障正常用户数据带宽。为确定引发 VLAN6 广播数据的具体原因并排除，故障定位具体步骤如下。

首先远程登录核心交换机，输入命令“display vlan 6”，发现 G0/0/11 ~ G0/0/16 划分在 VLAN6 下。6 个端口分别连接 6 个位置的汇聚交换机，其中 11、12 号端口下挂的是财务科和人力资源部的两个汇聚层交换机。使用命令“display arp vlan 6”查看交换机自动学习到在线的 VLAN6 主机 MAC 地址，发现其中一台主机的 MAC 地址学习错误。根据以往经验，该网络中可能存在环路。

依次对这 6 个端口运行 shutdown 命令，并检查网络的状态。最终发现在 12 号端口关闭，其他端口开启时，VLAN6 的网络恢复正常，将故障范围压缩到 12 号端口下连网络。

来到 12 号端口下挂的汇聚交换机现地查看，发现所有端口的绿色指示灯闪烁过快，数据交换不正常，采用上面的故障排除法将故障定位到其中一根网线端口。进一步检查发现网线连接的交换机与汇聚交换机之间存在环路。该交换机下的两个墙线接口同时连到了一个交换机。去除多余的线路连接，再开启核心交换机 12 号端口，VLAN6 所有端口的网络恢复正常。

故障排除

由于网络环路会引起数据无休止地在交换机各个端口中重复转发，引起广播风暴，导致网络故障。为了防止类似的故障再次发生，笔者在核心交换机端口下启用端口环路检测功能，当然也可以配置在汇聚交换机。该功能可以自动关闭有环路的端口，自动隔离环路，保护其他端口下网络正常。在交换机全局模式下，具体配置如下：

// 在交换机中启用环路检测功能；

```
[H3C]loopback-detection enable
```

// 设置交换机环路检测时间间隔 10 秒；

```
[H3C]loopback-detection interval-time 10
```

然后，进入相应的交换机端口下，运行命令：

// 在交换机端口中启用环路检测功能；

```
[H3C-GigabitEthernet0/0/12]loopback-detection enable
```

// 在交换机中启用环路端口自闭功能；

```
[H3C-GigabitEthernet0/0/12]loopback-detection action shutdown
```

上述命令表示端口探测到环路时会被关闭。交换机自动关闭端口后，端口状态为（loop down），表示因为环路而关闭。

注意

在 H3C 5500S 等低系列交换机中,使用端口环路关闭功能时,一旦网络中出现环路端口会自动关闭,网络环路故障解决后需手动启动端口。

经验总结

通过这一次网络环路故障的定位与排除,可以看出排除这类故障通常需要进行以下几个步骤:首先,通过交换机指示灯的闪烁状态和 MAC 地址学习情况判断

网络是否存在环路故障;如果确定存在网络环路,先通过核心交换机,确定故障 VLAN;再通过 VLAN 确定有问题的端口;在端口下进一步确定相关的接入交换机,依次类推直至找到具体的故障点,根据故障原因,排除故障。

为了避免某个端口的环路故障引起整个 VLAN 甚至整个网络故障,笔者建议在结构相对简单的网络中,最好开启交换机端口的环路检测功能。在结构相对复杂的网络,比如多个核心交换机相互备份、负载均衡的网络中,可以启用 STP 协议来消除网络环路。

超大硬盘服务器安装记

广州 张鹏

笔者因单位配发的存储设备迟迟未能到位,为保证数据备份工作的顺利进行,笔者决定采用大硬盘文件服务器作为临时的数据存储解决方案。升级原有浪潮服务器,并增加独立 Raid 卡,以 8 块 2TB 硬盘构建大容量的数据备份服务器。

将硬件设备接好后,首先对 Raid 卡进行配置。将 8 块硬盘均添加到 Drive Groups0 中。选择 Raid6 方式构建逻辑磁盘,磁盘容量达到 $1.818 \times 6 = 10.908\text{TB}$,并提供两块硬盘的校验功能。

相比 Raid1 损失一半的磁盘空间,Raid6 磁盘空间利用率明显更高。Raid6 最多允许两块硬盘同时发生故障,相比于 Raid5 也能提供更高级别的容错等级。

作为文件服务器,稳定高效是关键。笔者决定选用 64 位的 RedHat Linux 6.2 作为文件服务器操作系统。

故障现象

由于此前使用的服务器硬盘空间较小,缺乏在大容量磁盘空间环境下安装服务器的经验,所以只能摸索着开始安装。当进行到磁盘分区时,问题出现了,系统安装引导提示只能使用不超过 2TB 的磁盘空间。

故障分析

在网上查了一下,原来这都是 MBR 格式的文件系统所引起的。MBR 方式的文件系统受寻址能力限制,只能支持不超过 2TB 的磁盘空间。要加载超过 2TB 的磁盘空间,需要采用更加先进的 GPT 模式。

笔者最初的想法是,首先在较小的磁盘空间内先安装操作系统,待系统启动后,再到 Linux 环境下挂载剩余空间。可是实际操作过程中,发现剩余磁盘空间仍处于逻辑硬盘 sda 上,在使用 parted 进行 GPT 格式转换时,由于 sda 磁盘正处于激活状态,无法进行,所以也无法挂载剩余的磁盘空间。

故障解决

既然已经弄清楚了问题的由来,接下来的就是如何解决这一问题了。一种方法是在安装系统时采用 GPT 方式管理磁盘空间。可是在 RedHat Linux 的图形安装引导中,笔者没有找到如何进行配置,只好暂时放弃这一方案。第二种方法是构建两个逻辑分区。一个小于 2TB 的分区正常安装操作系统,另一个超大分区以 GPT 方

式挂载到操作系统中去。第二种方法除了可以解决超大分区加载的问题外，还可以将操作系统和数据盘分开，更加有利于文件服务器的维护和管理。

配置详解

按照第二套思路，首先修改 Raid 配置。在原有 Raid6 驱动器组的基础上，进一步将逻辑驱动其分为两个虚拟磁盘 VD0 和 VD1。其中 VD0 配置大约 500GB，用于安装 Linux 操作系统。剩余的磁盘空间留给 VD1，用于数据存储。

在虚拟磁盘 VD0 上安装操作系统后，登录到 Linux 中，发现系统包含 /dev/sda 和 /dev/sdb 两个磁盘。其中磁盘 sda 中 sda1 分区挂载到了 /boot 下，sda2 挂载到系统根目录中。此时虽然能够看到 sdb 的容量在 10TB 左右，但是在将文件格式转为 GPT 前，该分区还无法正常使用。由于 fdisk 不支持超过 2TB 的磁盘空间的管理，需要使用 parted 分区工具进行分区管理。

执行“parted /dev/sdb”进入分区工具中，执行“mklabel gpt”，将 sdb 改成 gpt 大分区格式。再执行“mkpart primary 0 -1”创建新的分区。新分区信息如图 1 所示。

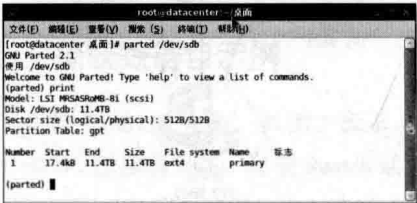


图 1 GPT 分区信息

接下来就是格式化分区“mkfs.ext4 -F sdb1”，并将格式化好的分区 mount 到指定的位置。为了每次系统启动时 sdb1 分区能够自动挂载，还需要在“/etc/fstab”中添加对应的分区信息。这样每次启动后，一个 10TB 大小的分区就可以被访问了。

经验总结

采用 GPT 是源自 EFI 标准的一种较新的磁盘分区表结构的标准。与 MBR 分区方式相比，它突破了 4 个主分区的限制，每个磁盘最多支持 128 个分区。支持大于 2TB 的分区，最大卷可达到 18EB，非常适合超大存储空间的管理。EXT4 文件系统容量达到 1EB，而文件容量达到 16TB，这是一个非常大的数字了。

IT 硬件性能的提升，除了带来更快的处理速度、更大的存储容量外，对系统安装、配置和管理也有了新的要求，同时也要求从业者的知识和经验能够同步更新。只有真正做到与时俱进，才能在工作中提高效率，少走弯路。



用交换机捕获数据排障

福建泉州 王刚 曾玮琳 郑洪飞

随着信息技术的快速发展，包括互联网在内的各种网络所承载的业务也越来越复杂，遇到的故障类型也越来越多样化，排除故障的难度逐步增加。现在常见的网络故障一般都需要通过捕获数据包进行故障原因分析和故障点定位。如何快速捕获数据数据包并对数据数据包

进行分析，以达到快速定位和排除网络故障呢？本文对常用的几种网络捕获数据包环境和捕获数据包方式进行说明，并引出这种实用但不常用数据包捕获方式——交换机自主捕获据方式，重点介绍这种捕获方式的特点，并以华为交换机为例，介绍如何配置并捕获数据数据包。

数据包捕获环境与方式

1. 主机环境

主机环境是主机直接接入外部网络，链路未接入集线器和交换机，一般是利用捕获数据包软件对进出主机的网卡的数据包进行捕获（如图1所示）。这种方式只能对本主机的数据包进行捕获。

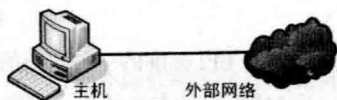


图1 主机环境

2. 集线器环境

在集线器环境，局域网内的主机都属于同一个冲突域，集线器会泛洪所有的数据包，所有主机均可以接收到局域网内的数据包。这种环境一般是在局域网核心交换设备为集线器（如图2所示），当主机1给主机2发送数据时，集线器会将数据包也转发给主机3。目前，除特殊需求外，已很少能遇到这种网络环境，这种方式是捕获的数据包过多，筛选量过大，捕获效率不高。

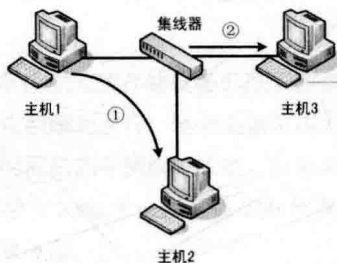


图2 集线器环境

3. 交换机环境

交换机环境是目前主流的局域网拓扑结构，局域内除组播和广播包外，其他的数据包除相关主机可以接收到外，其他的主机是无法接收到这些数据包的（如图3所示），主机1给主机2发送数据时，主机3是无法接收到这些数据的，如果要捕获这种数据包，需要特殊的手段和方式。

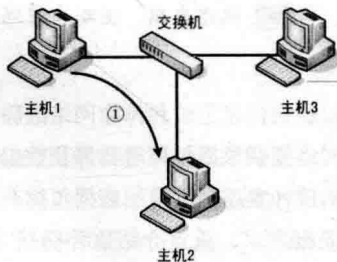


图3 交换机环境

在交换机环境下，一般使用端口镜像、ARP欺骗、MAC地址泛洪、加装分流器和更换交换机为集线器等方式进行捕获数据包。端口镜像捕获方式是在交换机上进行端口镜像配置，将要捕获的端口数据包流量全部镜像至捕获数据包的端口，从而捕获数据包。这种方式会增加交换机压力和网络流量，也是目前最常用的捕获方式。

ARP欺骗方式是使用ARP欺骗攻击来捕获数据包（如图4所示），正常主机2给主机3发送数据，主机3给主机2发回数据，跟主机1没有任何关系。但主机1要捕获主机3发送给主机2的数据包，主机1就会发送ARP欺骗攻击包，告诉主机3IP地址为IP2的MAC地址为MAC1，同时，告诉这样就会毒化主机3的ARP表，主机3的ARP表中IP地址为IP2的MAC地址为MAC1而不是MAC2。这样，主机3发送给主机2的数据就会被转发给主机1，在主机1捕获这些数据后再视情况决定是否将数据再转发给主机2，这样也就可以捕获数据包了。这种方式会影响主机2和主机3之间的正常通信，是一种零成本的抓包方式，当数据过多时，会造成数据丢失，捕获效率不高。

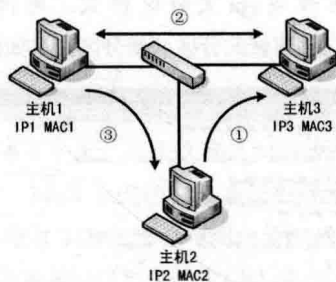


图4 ARP欺骗

MAC地址泛洪方式也是一种零成本的捕获方式，主机1要捕获主机3和主机2之间的数据包，主机1会泛洪大量的无效MAC地址，从而极大地充满交换机的MAC地址表，而主机2和主机3的MAC地址无法存入交换机的MAC地址表，这时，当主机2和主机3进行通信时，就会广播自己的数据包，这样主机1就可以捕获这些数据包。这种方式会极大地影响网络中的通信质量，捕获效率也极为低下，容易造成新的故障点。

加装分流器类似端口镜像，也是比较常用的一种捕获数据的方式，分流器可以实现对输出接口上的数据的镜像和复制，一份给正常的通信对象，复制的一份给捕获主机，这种方式需购买分流器，成本较高。更换交换机为集线器也可以捕获数据包，但会造成网络通信质量下降。

交换机自主捕获方式

无论是哪种捕获环境或是捕获方式，都存在一定的不足，为提高捕获效率，这里推荐一种实用的捕获方式——交换机自主捕获据方式。

这种捕获方式相比较其他几种常用的数据包捕获方式，有几种优势：

一是使用该功能可以简化报文分析设备和网络监控设备的部署，不需要将网络环境进行改造，不需要购买额外网络设备，不会中断现有网络通信，不会造成网络通信质量严重下降。比如，不需要将交换机更换为集线器，不需要将交换机的光接口转换为电接口，不需要购买分流器。

二是在设备上配置报文捕获功能后，可以配置相应的过滤规则，对数据包进行过滤，只捕获需要的数据包，而不是捕获所有的数据包，可以在命令行配置终端界面上查看捕获的报文，极大地提升了维护效率，降低了维护成本。

三是可以将捕获的数据包上送到远端 TFTP 服务器或 FTP 服务器，由主机进行分析，可实现捕获和分析同时进行，捕获效率极高。

交换机自主捕获数据包示例

以华为交换机 S2750 为例，如图 5 所示，Switch 通过接口 GE0/0/1 连接到网络。捕获 Switch 通过接口 GE0/0/1 的所有上行业务报文捕获，并 ACL2000 的报文

上送到 FTP 服务器 100.0.0.1，FTP 用户名为 user，密码为 123456，并将捕获的报文保存到 capture.cap 文件中。在配置报文捕获功能时，需要先配置 ACL 规则，用来捕获指定 ACL 编号规则的报文。本例中，以 ACL 的编号为 2000。



图 5 拓扑结构图

1. 操作步骤

- (1) <HUAWEI> system-view
- (2) [HUAWEI] sysname Switch
- (3) [Switch] capture-packet interface gigabitethernet 0/0/1 destination terminal packet-len 128
- (4) [Switch] capture-packet acl 2000 destination ftp-server 100.0.0.1 username user password 123456 file capture.cap

进入交换机系统视图，capture-packet 命令用来在设备捕获符合设置规则的业务报文，并上送到终端显示，或保存到本地，也可以发送到远端 FTP/TFTP 服务器。

2. 不足之处

目前只支持捕获上行方向报文，不支持捕获下行方向报文。某个时刻只能有一个捕获报文实例，即前一次捕获报文流程没有结束，不能启动下一次捕获报文。捕获的报文有速率限制，缺省值是 64kbps，如果有突发流量，超过捕获报文的速率限制，可能会存在丢数据包现象。

❖ 滥用飞秋网堵塞

▼ 新余 刘秋根

飞秋（FeiQ）是一款免费的局域网聊天传送文件的绿色软件，不需要服务器支持，具有局域网传送方便，速度快，操作简单等优点，同时具有 QQ 中的一些功能。正因如此，飞秋在笔者单位内网得到了广泛的应用，用户数以万计。然而在给大家带来便利的同时，也出现了一些问题。例如，滥用飞秋的一些功能，引起内联网广

域网线路堵塞，影响正常的业务系统在网络上运行。

故障现象

前不久，笔者单位就发生了数起因飞秋使用不当而引起的业务网广域网线路堵塞故障。故障现象表现为业

务网的业务办公专线通讯开始变得非常慢，到最后基本不通。登录路由器查看业务办公专线物理端口和协议均正常，但 Ping 不通对端网络，而此时和业务办公专线相互热备的专线通讯正常。

故障解决

第一次出现此故障时，由于技术条件限制和缺乏经验等原因，故障定位排查工作一波三折，走了不少弯路。开始以为是一般的网络设备硬件故障，依次尝试了重启网络设备、更换专线光转接头、ATM 接口卡、更换专线光缆以及重新配置专线数据等，都没能解决问题。后来，在相关各方参加的问题分析会上，专线运营商提出故障发生时在数据机房监测到该专线流量偏大，有些异常，准备将 2M 专线带宽暂时提高到 3M 测试线路能否正常。

考虑到可能是网络流量引起的故障，我们启用了 NetFlowAnalyzer 7.6 网络监控软件监控网络线路流量。果然，当第二次故障发生时，通过 NetFlowAnalyzer 7.6 监测到业务办公专线的峰值流量远超 2M，甚至达到 10M 以上。在检查具体的流入、流出数据源时，发现有几个异常大流量的数据源，而且数据流都是使用 UDP 2425 端口数据，很明显是飞秋产生的数据流。断开异常数据源 IP 客户端，线路通讯很快恢复正常。

规范使用飞秋

知道了滥用飞秋可能引发内联网广域网线路通讯堵塞问题，我们可以采取以下一些针对措施，预防问题的发生。

1. 限制飞秋的使用时间和使用范围

如在年终结算等关键时段禁止使用飞秋，限制飞秋在辖内使用等。

统一飞秋软件版本；规范飞秋的设置，禁用一些占用大量流量资源的不必要的设置，如：禁用系统设置里的自动检查最新版本；禁用功能设置里的上线时通知其

他用户、下线时通知其他用户、其他用户上线时进行通知、其他用户下线时进行通知、允许其他用户得到我的好友列表信息、自动刷新选项等；禁用个性设置里的聊天对话框右上角显示 Web 内容（天气预报）、获取资讯信息等；禁止在网段与好友 IP 设置里添加除中支辖内外的整个其他网段好友 IP。

2. 实时监测网络流量

在线路流量发生异常时及时发出报警信息。我们采用了 NetFlowAnalyzer 7.6 网络监控软件，它能够实时整个监控网络线路数据流量，并在线路流量发生异常时及时发出报警信息，而且能够显示具体的流入、流出数据源 IP 及相应的流量，使得能够快速定位有问题的数据源 IP，以便采取相应处理措施（如断开流量异常的数据源）使线路通讯恢复正常。

3. 进一步更新规范内联网 QoS 定义

尽量将所有最新的相关应用 IP 分别归入 Real (ef)、Capital、Interaction、OA 和 Test (af) 类，而将飞秋等即时通讯软件归入 Default (be) 类，限制飞秋软件通讯对带宽的占用，优先保障 Real (ef)、Capital、Interaction、OA 和 Test (af) 类等业务应用系统网络通讯需求。

4. 删除占用流量的功能

使用订制版的飞秋或其他类似即时通讯软件，也可对飞秋软件进行二次开发，删除其中不必要的占用大量资源和流量的功能。

5. 禁止飞秋等即时通讯软件的使用

可以在 H3C 客户端准入策略服务器上禁止飞秋程序的运行，也可以在网络核心设备上定义飞秋访问控制列表，禁止飞秋数据的传送。

例如在核心交换机上定义如下访问控制列表禁止飞秋数据传送：

```
acl number 3002 name deny-feiq
rule 10 deny udp destination-port eq 2425
rule 20 deny tcp destination-port eq 2425
rule 30 deny udp source-port eq 2425
rule 40 deny tcp source-port eq 2425
```

❖ 关注交换机版本

北京 解佳金 张颖 陈万雨

单位为实现总部与各分散下属单位召开视频会议，根据需要先后采购了3套视频会议系统，在总部中心机房利用3台华为S5700交换机分别作为3套系统的接入交换机，进行连接入网。同时，利用现有的运维管理系统对新入网的3台交换机进行了监测。网络结构如图1所示。

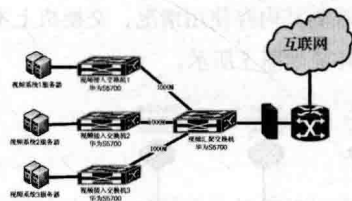


图1 视频会议系统网络组织图

故障现象

某天，最先投入使用的视频会议系统在一次使用中突然出现画面中断，现场保障人员迅速到机房查看系统运行情况，发现是网络连接中断导致。由于查看及时，还观察到了该视频会议系统的接入交换机正在进行重启。随即排除了线路的原因，将排查的重点定位在华为S5700视频接入交换机上。约5分钟后，交换机重新启动，并恢复了视频会议系统的业务功能。

由于事先将该交换机纳入了运维系统的监测管理，运维系统通过SNMP主动向交换机轮询采集各种数据，同时交换机也通过trap配置，适时向运维服务器发送trap事件。就在故障发生的同时，在运维系统的监测画面中也出现了该交换机发生linkdown事件的告警，由此更加断定确实是由于交换机故障才导致的视频会议系统中断。

故障分析

故障发生后，单位组织技术专家对问题交换机进行

分析，先后查看了交换机日志，并没有发现异常的告警，之后又查看了交换机的其他配置，也没有发现问题，故障前也没有出现丢包等不正常现象。就在调查进行了2天后，终于在运维管理系统的一项数据统计中发现了端倪。

通过运维系统，在对该交换机各类数据近一个多月的分析中发现，内存利用率在发生故障时为91.003%，进一步查看历史数据，发现5月1日的内存使用率为61.267%，每天内存利用率以07%~1%的速度单调递增，历时33天，达到峰值91.003%，随后发生了交换机重启（如图2和图3所示）。至此，故障确诊为交换机内存溢出，引起重启，最终导致故障发生。



图2 视频交换机一个月的内存变化曲线



图3 故障发生时的内存监测曲线

（备注：运维系统每3分钟采集一次，以上数据为每天晚上8点整的瞬时内存利用率。）

交换机自动重启后内存利用率恢复为56.994%，3天后又上升为59.626%，仍然在按照之前的单调递增规律，每天不断累计内存。此外，在对另外2台视频接入交换机的内存利用率统计时，也发现了同样的变化趋势。为防止故障再次发生，当利用率达86%时，对交换机进行了计划重启，暂时延缓了故障的发生。

在涉及视频会议系统的4台交换机中，型号

均为华为 S5700，其中汇聚交换机 1 台，版本为 V100R005C01SPC100，未出现类似的故障现象，接入交换机 3 台，版本为 V200R001C00SPC300（2012 年 6 月版本）。会不会是后者的系统版本存在内存溢出的漏洞导致的呢？带着这个疑问，笔者查阅了华为官方网站相关信息，自 2014 年底以来，华为交换机通告了有关该问题版本的部分漏洞，会导致内存溢出。经与华为客服的工程师联系沟通，得知曾经在其他单位也遇到类似问题（内存使用率单调递增）。由此，故障原因可以确定是交换机的 IOS 版本存在隐患。

为进一步深入分析内存溢出的原因，请来了华为公司设备研发工程师对故障现象进行确认，并协助调查故障原因，从故障交换机的系统版本入手，进行查找问题。

1. 确认当前交换机型号及系统版本，现网华为 S5700 设备为 v200r001c00spc300，加载补丁 V2R1SPH002.PAT，交换机作为一个二层设备使用，无特殊配置。

2. 查看日志，没有看到导致设备内存升高的信息。

3. 查看 MAC 漂移信息，没有看到有 MAC 漂移记录，dis mac-address flapping record。

4. 查看攻击报文的统计数据，只有 icmp-flood 有计数增长。因为运维服务器在一直 Ping 交换机，所以该项有计数增长是正常的，display anti-attack statistics。

在分析了所有可能的问题后，开始怀疑存在运维管理系统和被管交换机之间的配合存在问题，通过命令行：

display inspect mem-debug-info 29 0 0 0

发现设备内存的 BLK1024 字节的内存大量占用，而且不断累加，没有正常释放。通过反复实验，原来是运维管理系统在进行 SNMP 采集轮询中，当获取 IPv6-TCP-MIB 中 ipv6TcpConnTable（OID：1.3.6.1.2.1.6.16）的任意节点时，交换机对申请的配置消息内存未做释放处理，导致出现 1024 字节内存泄漏（如图 4 所示）。



图 4 IPv6-TCP-MIB

试验验证

1. 实验环境

为进一步验证华为 S5700 系列交换机在内存性能方面存在的隐患问题，我们搭建了实验环境，分为两个部分：

（1）对交换机加运维管理系统进行测试：将相同型号、相同版本的 3 台华为 S5700 交换机与 2 台运维管理服务器组成一个局域网（如图 5）。其中一台加载最新的 SPH018 补丁，另一台升级版本为 Version 5.130（S5700 V200R003C00SPC300），第三台保持原始版本不变。这三台交换机均配置 SNMP，并利用运维管理系统进行监控。三台交换机上均没有加载任何业务。

（2）对原始版本不加运维管理系统进行观测：将一台华为 S5700 交换机直接与一台计算机利用 Console 线相连，用于观测其内存使用情况，交换机上不加载任何业务。测试环境如图 5 所示。

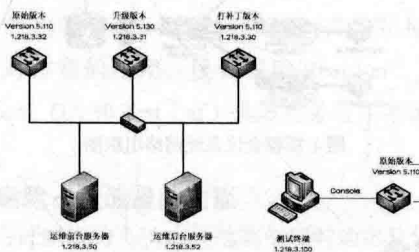


图 5 华为 S5700 系列交换机内存溢出验证测试拓扑图

2. 测试结论

在测试环境中，未升级版本的 3 台交换机开机后，初始内存利用率均为 57%，升级版本后的 1 台交换机开机后初始内存利用率为 48%。7 月 3 日至 7 月 13 日，10 天内我们均定时对交换机内存使用率进行采集，不同条件的交换机内存增长曲线图如图 6 所示。

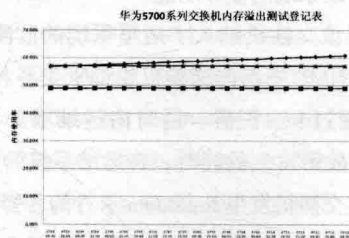


图 6 华为 S5700 系列交换机内存溢出试验测试登记表

分析以上测试结果可以得出以下结论：

（1）版本为 Version 5.110（S5700 V200R001C00SPC300）的华为 S5700 系列交换机，会在网管系统的采集触发下出现内存利用率单调递增的现象。

(2) 版本为 Version 5.110 的交换机加载 SPH018 补丁后, 内存使用率保持稳定在 57% 左右, 不再单调递增。

(3) 版本为 Version 5.110 的交换机在进行整体 IOS 版本升级后, 内存使用率较升级前降低了 8%, 并保持稳定在 48% 左右, 未出现利用率单调递增的现象, 但升级后 CPU 利用率较升级前上升了 5%。

故障启示

网管人员在网络维护过程中, 不应只关注端到端的

网络状态, 组成网络的各个网元设备的性能, 更需要定期进行经常性的预检维护, 将各种故障和隐患的苗头解决在萌芽状态。当然, 要进行分析就必须依托现代化的运维管理平台, 进行自动的数据采集、传输和存储, 并根据需要产生相应的报表, 方便网管人员进行预测分析。在分析过程中, 要善于运用各种手段进行多角度验证, 确保分析的结果真实可靠。

被 “*” 感染的 IP

湖北 杜致远

单位网络使用传统的大二层网络结构, 用户通过楼栋交换机直接接入网络中心汇聚层设备, 再接入到核心设备, 核心设备上接计费系统、防火墙等设备为用户提供上网服务。

故障现象

某日, 接到下面办公室老师的电话, 反映无脑无法上网, 网卡显示正常, 我的电脑 Ping 该电脑使用 IP 地址正常, 登录时超时。首先判断是用户的电脑有问题, 告诉用户是个人电脑出现故障, 有程序阻挡了客户端软件的运行, 让用户自己检查电脑, 实在不行的话, 就重装系统。

更换 IP 临时解决

过了一天用户又打电话, 反映系统重装后, 客户端还是登录不了, 请求现场处理。到达用户那里, Ping 网关正常, 客户端登录显示超时。再 Ping 计费系统 IP 显示超时, 电脑到计费系统不通。更换 IP 地址后再 Ping 计费正常, 登录正常, 故障排除。

故障排查

回到办公室将刚才那个有问题的 IP 地址设置在另外一台电脑上, 再 Ping 计费系统显示超时, 难道这个 IP 地址有问题? 再换一台电脑故障依旧。联系厂商工程师, 让在核心的上行口 (与计费互联口) 做端口镜像, 使用 Wireshark 软件进行数据采集, 采集条件是该问题 IP 地址, 然后再用一台电脑设置成问题 IP 地址 Ping 计费系统, 采集软件没有采集到任何跟该 IP 有关的信息, 说明核心设备并没有将该 IP 有关的数据包提交过来, 说明核心设备上面出现了问题。

再联系厂商硬件工程师进入硬件后调试界面, 发现核心设备第一块业务板里面有许多出错信息, 说明该业务卡有问题。用 `show arp | in "IP"` 命令后, 出现如图 1 所示信息, 该 IP 前面多一个 “*”, 说明该 IP 地址在写入 MAC 地址表项时出现了问题, 属于硬件故障, 需要更换该业务板。

故障排除

联系厂商发来备件后更换此卡后, 该 IP 的电脑上网认证正常, 再用 `show arp` 命令查看该地址表项时, 前面没有带 “*”, 故障排除。

ARP (Address Resolution Protocol) 即地址解析协议, 是将设备的 IP 地址与 MAC 建立对应联系, 是网络传输的基础, 对应的 IP 地址表项如果出现了问题, 就会造

成网络不通。本次故障就是由于硬件故障造成表项异常, 使得个别数据异常, 引起用户上网故障。

修复交换机系统文件

广州 杨永刚 黄振兴

ZXR10 5928E 是中兴推出的全千兆中型以太网交换机, 该机功能丰富, 性能稳定, 在各类数据中心和网络机房应用广泛。近期单位机房发生一起断电事故, 导致多台服务器断。经查, 这些服务器都连接了同一台 5928E 交换机, 因此初步判断为交换机故障。使用串口线登录交换机, 发现该交换机提示提取 “/img/zxr10.zar” 失败无法启动, 并反复重启, 由此判断该交换机可能因断电导致系统文件丢失。下面将系统文件的恢复方法进行介绍。

获取系统文件

一般地, ZXR10 5900E、3900E、3900A 系列交换机的 Flash 中包含 img、cfg、data、lost+found 四个文件夹, 其中 img 文件夹下存放系统文件, cfg 文件夹下存放用户配置文件, data 文件夹存放日志文件。在全局模式下, 通过 dir 命令可以查看各个文件夹下存放的内容 (如图 1 所示)。

```
ZXR10#dir img
Directory of flash:/img
```

	attribute	size	date	time	name
1	drwx	2048	Jun-26-2014	10:30:55	..
2	drwx	2048	Jan-01-2000	07:28:16	..
3	file	16020020	Jan-01-2000	07:28:29	zxr10.zar

264241152 bytes total (247025664 bytes free)

图 1 查看各个文件夹下存放的内容

获取系统文件 zxr10.zar 有两种方法, 一种是向中兴官网或客服索取, 另一种是从正常运行的交换机中上传导出。

从交换机中导出系统文件的方法如下:

1. 架设 FTP 服务器 (假设服务器地址为 192.168.1.2, 用户名密码都是 target)。
2. 远程登录交换机, 在全局模式下, 启动上传命令。

需要注意的是, ZXR10 5900E 系列交换机除了正常的业务网口之外, 还配置了一个相对独立工作的管理网口, 这两类网口上的上传命令是不同的。

使用业务口拷贝系统文件的命令如下:

```
ZXR10#copy flash: /img/zxr10.zar ftp: //192.168.1.2/
zxr10.zar@target:target
```

用管理口拷贝系统文件:

```
ZXR10#copy flash: /img/zxr10.zar ftp: mng
//192.168.1.2/zxr10.zar@target:target
```

文件 zxr10.zar 大小约为 16MB。因为两种方法分别采用了不同的存取机制, 实践表明, 通过业务口拷贝系统文件大约需要 15 分钟, 而通过管理口拷贝系统文件大约只需要 2 分钟, 因此建议网络管理员使用管理网口拷贝系统文件。

使用之前, 需要对管理口的地址参数进行设置。

```
ZXR10 (config) #nvram mng-ip-address 192.168.1.1
255.255.255.0
```

```
ZXR10 (config) #nvram default-gateway
192.168.1.254 255.255.255.0
```

对业务口进行地址配置即采用一般的 VLAN 划分的方法, 不再赘述。

网络启动

故障交换机由于系统文件丢失, 不能从 Flash 中加载启动系统, 因此改用通过网络启动。

1. 架设 FTP 服务器 (服务器地址为 192.168.1.2, 用户名密码都是 target), 将系统文件存放于 FTP 服务器的根目录下, 服务器网口与交换机管理口直连。需要注意

的是，网络启动对 FTP 服务器有较高要求，经测试，多款 FTP 软件都加载失败，判断网络启动不支持分块 FTP 传输，这里推荐使用 3CDaemon 和 wftpd 两款 FTP 服务器软件。

2. 在交换机上设置网络启动参数。

```
Hit any key to stop auto-boot: 0
[boot]: c
'.' = clear field; '-' = go to previous field; '^' = quit
Boot Location [0:Net, 1:Flash]: 0
//0 为从后台 FTP 启动，即网络启动
Client IP: 192.168.1.1
// 对应为网络管理接口地址，此 IP 仅 BOOT 下生效
Netmask: 255.255.255.0
Server IP: 192.168.1.2
// 对应为后台 FTP 服务器地址
Gateway IP: 192.168.1.2
// 网关地址指向 FTP 地址
FTP User: target
// 对应为 FTP 用户名 target
FTP Password:
// 对应为 target 用户密码
FTP Password Confirm:
Boot Path: zxr10.zar
// 网络启动注意配置启动路径为 zxr10.zar
Enable Password:
// 使用缺省
Enable Password Confirm:
// 使用缺省
3. 启动
执行引导启动操作。
```

```
[ZXR10 Boot]: b
// 启动交换机
正常启动后出现全局模式界面：
ZXR10>
```

下载系统文件

由于上述启动过程为网络启动，Flash 中仍缺少系统文件，需要通过业务口或者管理口下载启动文件 zxr10.zar 至交换机的 Flash:/img 目录。

业务口命令：

```
ZXR10#copy ftp: //192.168.1.2/zxr10.zar@target:target
flash: /img/zxr10.zar
```

网管口命令：

```
ZXR10#copy ftp: mng //192.168.1.2/zxr10.zar@
target:target flash: /img/zxr10.zar
```

与获取系统文件相类似，下载系统文件采用通过管理口比通过业务口下载速度要快得多。

修改交换机启动项设置

将设备启动方式从网络启动改为本地启动：

```
ZXR10 ( config ) #nvram imgfile-location local
ZXR10 ( config ) #exit
ZXR10#write
```

重启交换机，使用 reload 命令重启交换机，也可以通过按设备后面的电源开关重启。交换机正常启动恢复运行。

经过考察，通过管理口恢复交换机 IOS，传输速率更高，系统恢复速度更快，普遍适用于安装有 mng 管理口的各型号中兴路由交换设备。

低版本引发路由器重启

福建泉州 王刚 曾玮琳 郑洪飞

故障现象

单位有一台华为 AR3260 路由器，因业务需要拓展，新增了一块 2SA 单板，安装配置完成后，业务工作正常，但每隔几分钟路由器就会自动重启，因路由器承载业务非常重要，不得中断，无奈之下，先启用了备用路由器，然后对这台华为 AR3260 路由器的故障进行了排除。

引起路由器重启的主要原因

导致路由器自动重启的原因有很多，根据笔者多年的经验，发现主要有 4 种原因会导致或诱发路由器自动重启。

1. 硬件故障

硬件故障主要是核心模块和附属模块故障引发路由器自动重启，对于普通路由器或插槽较多的路由器而言，大部分的故障一般是主板、单板、风扇或电源模块故障造成，如单板与设备背板之间未插紧、电源模块接触不良会自动重启导致路由器自动重启、风扇模块发生故障等。

2. 软件故障

软件故障一般是由于配置不正确或使用系统版本问题，造成路由器自动重启，笔者碰到过一个因配置不当造成路由器自动重启的案例，管理员在低端路由器中使能了高端路由器的配置命令，而其实低端路由器并不支持此功能，造成路由器自动重启，因路由器操作系统版本基本通用，很多低端路由器可以使能高级路由器命令，但实际不支持此功能。

3. 网络流量异常

网络中因病毒、环路等原因导致数据流量非常多，导致路由器 CPU 负载增大，当超过路由器处理能力时路由器会自动重启。

4. 环境原因

因雷雨天气、环境温湿度超过路由器安全运行要求、

路由器外接电压不稳定、系统电源未可靠连接或周边电磁干扰严重、路由器灰尘较厚散热不良等环境原因，也会造成路由器自动重启。

故障分析

当路由器发生自动重启故障后，可以按照“先外部，后内部，先软件，后硬件”的原则进行故障排除。

1. 查看故障现象

查看路由器本身，除了自动重启外，只有风扇转速较快，噪音比平时要大很多，但各指示灯均正常。

2. 可能的故障原因

机房的温湿度均在正常范围，UPS 电源输出电压和频率均在正常范围内，路由器各指示灯均正常，但路由器出风口有积尘，初步判断，因增加板卡，热量增加，灰尘较多，造成局部散热不良而导致温度升高，造成路由器重启，如故障仍未解决，则可能是风扇配置错误或风扇模块故障，也可能由于网络内存在巨量数据包造成路由器 CPU 负责增加而重启，但这种可能性不大，因备份路由器工作正常。

故障排除过程

1. 打开路由器机壳，路由器主板表面、机壳出风口和风扇出风口存在很多积尘，使用小毛刷和吸尘器清理积尘后，又对风扇模块进行了检查，未发现异物卡住风扇叶片，用螺丝刀轻轻拨动风扇叶片，叶片转动良好，将风扇模块插入插槽并确保安装良好，上紧松不脱螺钉，启动后，各类指示灯正常，路由器依旧自动重启。

2. 进入路由器配置界面，路由器新增模块仅在串口配置了 IP 地址和在串口宣告了 OSPF 协议的网络，未使能其他命令。在用户界面输入 `display cpu` 命令，路由器未设置告警阈值，发现路由器 CPU 使用率不超过

10%，处在正常范围。在用户界面输入 `display fan` 命令，发现 3 个模块风扇转速均为 2940 ~ 2970，转速较高，增加模块后，热量增加，由于风扇采用智能调速策略，转速增加，也属正常原因，在用户界面输入 `display temperature all` 命令，发现各模块温度均正常，未发现异常。在用户界面输入 `display device` 命令，发现各模块运行均正常未发现异常，所有配置均正常，但路由器依旧自动重启，排除硬件和配置错误故障。

3. 在备用路由器上使用 `display interface` 命令，对所有接口的数据包进行了查看统计，发现所有的数据包均正常，数量流量均正常。在这种情况下，联系华为公司，其工程师建议对风扇的软件进行升级，在用户模式下输入 `display version slot fan` 命令，发现风扇软件版本为 103，版本较旧，华为公司的工程师提供了最新的风

扇软件，版本为 108（将软件的名称改为 `arfan.iap`），对风扇软件进行升级。

4. 先拔出新增的 2SA 单板，避免软件升级过程中，自动重启。

5. 启用路由器 FTP 功能，并将软件拷入路由器 Flash 中，然后在全局模式依次执行 `diagnose` 和 `upgrade fan-software flash:/arfan.iap` 命令，等待约 10 分钟后，风扇软件升级完毕，将新增的 2SA 单板插入槽位，开机运行，路由器运行正常，未出现自动重启现象，故障排除完毕。

路由器故障纷繁复杂，排错方法也不尽相同，但排错思路和原则基本一致。遇到路由故障时，网管人员需冷静分析，找出故障原因，及时排除故障。

❖ 辨识真伪网关

▼ 嘉兴 陈杰

二层网络是一个广播域，ARP 攻击就是通过伪造 IP 地址和 MAC 地址实现 ARP 欺骗，能够在网络中产生大量的 ARP 通信量使网络阻塞，攻击者只要持续不断地发出伪造的 ARP 响应包，就能更改目标主机 ARP 缓存中的 IP-MAC 条目，造成网络中断或中间人攻击。

ARP 攻击主要是存在于局域网网络中，局域网中若有一台计算机感染 ARP 木马，则感染该 ARP 木马的系统将会试图通过“ARP 欺骗”手段截获所在网络内其他计算机的通信信息，并因此造成网内其他计算机的通信故障。

故障现象

某园区网络不通，无法访问网页等应用系统，而汇聚交换机和局部接入交换机（不同 VLAN）交换机仍然能够被正常访问。网络结构如图 1 所示。

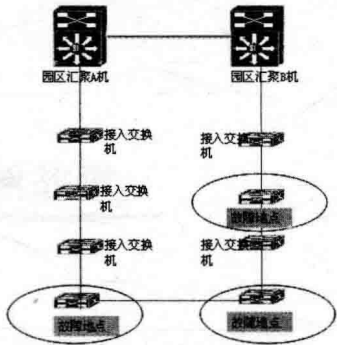


图 1 网络拓扑结构

故障排查

初步判断故障非硬件故障，而是存在于故障所处的 VLAN 内部。鉴于前几天该网段一直稳定运行，网络结构未曾改动，而且没有新增交换机设备。因此，网络内发生 ARP 攻击的概率极大。我们以此为据，开展故障排查工作。

1. 通过故障计算机的 ARP 表查找网关的 MAC 地址 b8-ac-6f-42-dc-08 (如图 2 所示)。

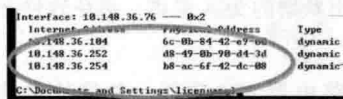


图 2 查找网关地址

2. 在网关所在的汇聚交换机上查找到网关的真实 MAC 地址 d8-49-0b-90-d4-30。发现两者不一致, 判断有伪造网关的客户端 (如图 3 所示)。



图 3 网关实际地址

3. 在网关所在的汇聚交换机上, 依据 MAC 地址, 查找假网关所在交换机端口。

4. 通过邻居发现协议, 发现伪装网关的客户端在某接入交换机上。

5. 在 binhaiscjd1_S3700 交换机上查找假网关 MAC, 发现伪装客户端在其 46 号口 (如图 4 所示)。

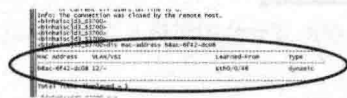


图 4 查找伪装客户端

6. 最终查找到这台电脑。经检查发现, 它的 IP 地

址被改成了 10.148.36.254 网关地址, 因此造成了模拟 ARP 病毒攻击的现象。在更换正确的 IP 地址后, 该 VLAN 所属网络段全部恢复正常。

故障分析

1. 在配置客户端 IP 地址时, 未通过网络管理员准确核实, 导致配置错误。

2. 使用者在客户端配置完错误地址后, 桌面上也曾弹出地址冲突, 但并未引起他的重视, 从而未及时与网络管理员联系, 导致了整个局域网无法跨越网关访问应用。

经验总结

在局域网中无法访问外部网络, 首先应判断客户端是否能到达网关, 若无法到达网关, 则需要检查接入交换机是否配置正确。若能到达网关, 则说明路由正确。然后再排查 ARP 表, 看是否有病毒或者 ARP 欺骗, 通过 MAC 地址定位到出问题客户端, 解决问题。

同时, 我们还必须加强信息网络安全宣贯, 严禁未经许可随意改变计算机网络配置, 引起类似网络故障, 影响整个网络的运行。

定位违规电脑

辽宁 冯志强 梁红星

故障现象

某日, 网络监测部门在互联网上通过监测终端, 发现我部局域网内某电脑连接了互联网, 并将该电脑的主机名、IP 地址、MAC 地址发给了我们, 责成我部尽快将其找到, 并上报相关情况。

公司为实现内部资源共享, 同时防止内部资料外流, 组建了专供内部使用的资源网。此网有专用的服务器、路由器、交换机、防火墙等网络设备, 与互联网物理隔离。内部电脑要上资源网需要安装实名认证软件。为防止人员将内部电脑连接互联网, 实名认证软件具有定时向资源网和互联网上监测终端发送主机名、IP 地址、网卡 MAC 地址等主机信息的功能。未进行实名注册的用户和主机 MAC 地址未在防火墙上绑定的电脑无法访问局域网外资源, 但可以访问局域网内部资源。

故障排查

为了找到该电脑，我们首先查看了 IP 地址所在的具体部门。因为单位的局域网由 8 个 C 类地址组成，主机数量很多。为了便于管理，在建网初期，已为各部门划分了不同的地址段。通过比对查找，发现虽然此 IP 地址属于甲部门，但确实不是该部门的电脑，肯定有人违规使用了其他部门的地址。看来从 IP 地址已经无法找到问题电脑了。

由于要访问局域网外资源网信息的电脑都在防火墙上进行了绑定，并有实名登记，如果此电脑曾经通过路由器出局域网，肯定绑定了 MAC 地址。于是将该电脑的 MAC 地址与防火墙中的 MAC 地址绑定表进行对比，也未找到相同的，看来又一个希望破灭了。

猜测该电脑可能还在线，Ping 该电脑的 IP 地址，但未能 Ping 通，看来不在线。经过大家的讨论和分析，认为此电脑如果是我单位某部门的，那么与此电脑同批采购的电脑的 MAC 地址的前几位应该是相同的。因为同一批次同一品牌的电脑所用网卡很可能是同一厂家的，其前 3 组用来表示网络厂商标识的 16 进制数应该相同。

故障解决

用局域网查看工具软件查看局域网内所有在线电脑

的 IP 地址和 MAC 地址，确实发现有两台电脑 MAC 地址的前几位与问题电脑相同。通过查看登记，这两台电脑也在同一个部门。于是我们直接前往该部门所在办公室，发现办公桌上有三台电脑，两台在用，一台关机。经过检查，问题电脑就是它。

原来，某人用 USB 线将手机与电脑相连，本来只想将手机内的照片传到电脑里，却开启了 USB 上网功能，导致内部电脑连接了互联网。

经验总结

问题电脑终于找到了，但问题还没有完，给我们留下了很多思索。为什么在局域网中定位一台内部电脑这么复杂？为什么会出现内部电脑外连事件呢？我想主要有三点启示：一是要规范内部电脑及其入网管理。每台投入使用的内部电脑都应登记在册，特别是 MAC 地址，并严格按划分的 IP 地址进行设置，不得使用非本部门的 IP。二是在技术方面，将每台入网的内部电脑 MAC 地址与对应交换机端口进行绑定，在交换机上进行相关设置，使未绑定的电脑无法入网。三是进行安全保密教育。不得将手机、无线网卡等可上网设备与内部电脑互联，防止因误操作导致违规上网。

❖ 软件引起的开机故障

广西桂林 周瑜

故障现象

前不久，办公室一台 2009 年出厂的华硕 F83S 笔记本出现故障。一开机还没有出现电脑自检画面就提示“Express Gate is Not Install on Your System or the Installation is Incomplete”，然后，按任何键都没有反应，包括 Ctrl+Alt+Del 也不管用，只有断电并卸下电池后再加电，才能再次开机。该提示为系统没有安装 Express Gate 或安装不完全。

故障排查

1. 排查硬盘故障，导致部分系统文件损坏或丢失（可能是 Express Gate 文件丢失）。拆下硬盘，挂在另一台笔记本电脑上，可以正常开机，说明硬盘无故障。

2. 排查软件故障。上网查询有关华硕 Express Gate 的相关信息，得知该软件为华硕电脑独有，是基于 Linux 开发的快速连接上网与使用 Skype 的环境，启动后只需要几秒钟就可以进入菜单，就能享用网络浏览、

聊天、听音乐等，而不需要进入操作系统，具有快速、安全、界面简单等优点。按照提示，也许安装 Express Gate 软件能解决问题。但是，无法进入操作系统，不能直接安装该软件。

3. 排查 BIOS 设置。在网上进行了搜索，有网友给出解决方法：在 BIOS 设置中把 Express Gate 关闭，也就是在 BIOS 里找到 Express Gate 选项，将 Enable 改为 Disable。可是刚启动电脑按 F2 准备进入 BIOS 时，电脑很快加载到该提示页面，经过多次操作故障依旧，根本无法进入 BIOS 设置界面，直接停留在提示画面。

另一种方法是拆下 COMS 电池，放电，或许可以解决。在拆 COMS 电池的过程中，比较复杂，不同于多数的笔记本，打开后盖很快可以找到。该款华硕 F83S 系列电脑的 COMS 电池，位于电源与光驱之间的主板内侧，基本将所有螺丝拧开，再拆下主板，方可取出电池，几乎将所有零件都拆下了，也许是出于产权保护吧。放电后，将电池装回，开机按 F2（未安装硬盘），终于可以进入了 BIOS。可问题又出现了，找了每一个菜单及选项，并没有 Express Gate 的设置选项，估计该故障的出现与 BIOS 设置无关。于是将 COMS 电池拆掉，不安装上去，再验证进一次 BIOS，可以顺利进入。

经分析，应该同时考虑 BIOS 和硬盘，将二者结合方可解决问题。于是安装上硬盘，可以顺利进 BIOS，但断电启动操作系统，依旧出现上述提示。看来，还是要先进入系统，解决 Express Gate 软件问题。

故障解决

首先做好准备工作，在网下载 Express Gate 软件，版本是 ExpressGate_VT32_64_090217 的压缩包。考虑到开机时看不到系统自检画面，分析可能是快速启动跳过了主板自检，而直接加载 Express Gate，先进入 BIOS，在 Boot 中关闭了快速启动。保存并退出 BIOS，

重新启动系统，依经验直接快速按 Esc 键，终于看到了进入 Windows 系统启动页面。进入系统之后，直接将下载的 Express Gate 解压默认安装。重启电脑，此刻电脑出现 NVRAM 加载成功，首先出现 Express Gate 系统界面，而后按 Esc 键后顺利进入系统。至此，该电脑故障解决。

故障分析

后来，对该机器仔细分析了一下启动情况。如果是断电冷启动，就会出现启动 Express Gate 界面，可以按 Esc 键取消，并进行 BIOS 的正常自检与引导启动，登录 Windows；如果是直接重启 Windows 或热启动，就会直接跳过加载 Express Gate，并进行 BIOS 的正常自检与引导启动，登录 Windows。该故障可能是机器加电开机，BIOS 启动引导后不进行自检，直接以某特定的方式寻找硬盘（或 U 盘、光盘）上的相关信息文件，并读入加载启动 Express Gate 所需文件，但因缺失关键信息文件而出现故障提示，不能跳过加载 Express Gate。对于带有 Express Gate 系统的电脑，要防止出现此类故障，可以先按电源开关然后在未加载前按 Reset 键或热启动组合键，或许可以解决不能开机问题。

经验总结

遇到故障时，多做准备工作。对出现故障的提示仔细分析，并在网上找资料看懂并争取弄透，再采取对应的措施处理。这次故障的出现到解决问题，处理者断断续续用了几天时间，没有仔细了解 Express Gate 是什么，更谈不上弄清楚 Express Gate 的启动原理，走了不少弯路。尤其在拆卸电脑 COMS 电池时，因经验不足，机器需拆卸的螺丝太多，花费了不少心思，还是在一位经验比较丰富的老同志的帮忙下才解决电池拆卸问题。

❖ 无效路由条目闹故障

福建泉州 王刚 荣世辉 程玉青

故障现象

笔者单位有同事反映向上级单位多次发送文件均失败，笔者第一时间怀疑该同事的计算机无法正常发送文件是由网线松脱、对应的交换机端口出现故障、计算机网卡出现故障、计算机 IP 地址特别网关设置错误等原因造成的。到了现场，笔者对可能的故障原因进行了一一排除，结果故障都不是这些原因造成的，遂进行了进一步的通断测试。一测试，却得到了有点“奇葩”的通断测试结果，而这些测试结果以前从来没有遇到过。

以下是笔者做的几项通断测试（通断测试主要使用“Ping”命令进行测试，为测试方便，特定义本级单位计算机编号分别为 B1、B2……，本级网关为 BG，上级单位计算机编号分别为 S1、S2……）。

1. 从该同事的计算机 B1（IP 地址为 36.130.20.11/22）Ping 本级网关 BG（IP 地址为 36.130.20.254/22），丢包率为 0，通。
 2. 从 B1 计算机 Ping 上级文件接收计算机 S1（IP 地址为 36.140.26.32/24）和上级其他计算机 S2（IP 地址为 36.140.26.34/24），丢包率为 100%，不通。
 3. 在 B1 计算机上，使用“route print”命令查看本机可以外连的网络信息，未查看到到达 S1 计算机的路由条目。
 4. 找其他同事的计算机 B2（IP 地址为 36.130.20.14/22）Ping 上级计算机 S1 和上级其他计算机 S2，丢包率为 0，通。
 5. 从计算机 B2 上 Ping 计算机 B1，丢包率为 0，通。
- 至此，出现了第一个比较“奇葩”的测试结果：同一网段的 IP 地址 Ping 异段同一目的 IP 网址，一个丢包率为 0，另一个丢包率为 100%，遂又进行了下面的测试。
6. 将同事计算机 B1 的 IP 地址更换为从未使用过的 IP 地址（36.130.20.16/22），然后分别 Ping 本级网关 BG，上级计算机 S1 和 S2，丢包率为 0，全通。
 7. 将其他同事计算机 B2 的 IP 地址更换为从未使用

过的 IP 地址（36.130.20.15/22），然后分别 Ping 本级网关 BG，上级计算机 S1 和 S2，结果可以 Ping 通本级网关 BG，但 Ping 上级计算机 S1 和 S2，丢包率为 100%，不通。

至此，又出现了第二个比较“奇葩”的测试结果：从未使用过的同一网段 IP 地址 Ping 异段同一目的 IP 网址，一个丢包率为 0，另一个丢包率为 100%，测试结果如表 1 所示。

表 1 测试结果

	网络节点	本级网关	S1	S2
第一次测试结果	B1（36.130.20.11/22）	通	不通	不通
	B2（36.130.20.14/22）	通	通	通
第二次测试结果	B1（36.130.20.16/22）	通	通	通
	B2（36.130.20.15/22）	通	不通	不通

造成网络异常的可能原因

针对测试结果，笔者首先对各网络节点进行了检查，均未发现故障。然后梳理了可能造成网络异常的一些可能原因。

1. 终端设置错误

这主要是终端用户对 IP 地址工作原理理解不清，随意设置和更换 IP 地址，造成 IP 地址设置错误，导致无法上网。还有可能是终端用户不设置网关 IP 地址或者网关设置错误，也是造成这种网络异常现象的原因之一。特别是很多单位从隔离广播风暴和网络安全考虑，会划分很多 VLAN，不同的 VLAN 其网关也不相同，有时一个办公室可能会有多个 VLAN，不同的计算机其 IP 地址范围和网关也会不同。笔者曾遇到过同一个办公室有三个 VLAN，而其中一台计算机设置成了其他 VLAN 的 IP 地址和网关，造成其无法正常上网。

2. 防火墙原因

很多单位在连接外网时，都会在网络入口处架设有防火墙，并根据业务和安全要求设置相应的防火墙策略，特别是对一些类似 BT、视频、QQ、其他敏感网络业务

端口和敏感的 IP 地址进行了过滤屏蔽。当终端用户使用的 IP 地址或业务系统端口被上级防火墙过滤屏蔽后,会导致用户终端无法访问该网络。当然,个人计算机的软件防火墙也有此功能,只是很少有人会专门去设置,一般都采用默认安全方式。

3. 网络设备配置错误

一般外连网络都需要路由器或三层交换机,如果网络设备配置错误,也会造成网络异常,但一般网络设备在配置完成后,都会进行测试,一般不会产生这种“奇葩”的故障现象,但也不排除这种可能性。

故障排查

笔者单位为末端网络节点,外连网络结构非常简单,对上级只有一条 2M 专线,使用基带 Modem 进行连接,在排除上级计算机 S1 未在软件防火墙中做特殊安全设置后,遂开始了故障排查。

1. 使用“ipconfig /all”命令检查了计算机 B1 的 IP 地址和网关设置,发现计算机 B1 的 IP 地址和网关 IP 地址设置均正确。在排除故障中,这一步很关键,因笔者曾遇到过一台计算机在感染病毒后,使用“本地连接→常规→详细信息”方式查看计算机的 IP 地址是错误的,而采用“ipconfig /all”命令方式查看 IP 地址和网关 IP 地址不会受病毒的影响。

2. 查看了本级硬件防火墙的策略,未对计算机 B1 做特别限制,后又询问上级单位防火墙的设置情况,上级网络主管单位在查看了防火墙的设置反馈说,并未对计算机 B1 进行特殊过滤屏蔽和隔离。

3. 笔者在 B1 计算机使用“tracert 36.140.26.32”命令查看 B1 到上级 S1 计算机的数据转发路径,发现数据包到了本级网关 BG 后,出现了一条为“36.130.254.11”的目的 IP 地址,之后全部为“请求超时”,无法到达目标网络(如图 1 所示)。

```
1 <1 毫秒 <1 毫秒 <1 毫秒 36.130.20.254
2 2 ms 2 ms 2 ms 36.130.254.11
3 * * * 请求超时。
```

图 1 “请求超时”信息

至此,笔者发现了问题所在,因为本单位对上级的网间网地址为“36.130.254.13/30”,而不是“36.130.254.11/30”,很可能是路由器表配置错误。

4. 登录路由器,进入特权模式,使用“display current-configuration”命令查看路由器中配置的路由条目,发现共配置了两条缺省路由(如图 2 所示)。

```
interface NULL0
ip route-static 0.0.0.0 0.0.0.0 36.130.254.13
ip route-static 0.0.0.0 0.0.0.0 36.130.254.11
```

图 2 查看路由器中配置的路由条目

因为本单位为末端网络节点,对外只有 1 条通信信道,从最小消耗资源角度考虑,笔者单位的路由器只需配置 1 条缺省路由即可达到通信要求。缺省路由是一种特殊的静态路由,指的是当数据包中的目的地址与路由表中没有相匹配的表项时,路由器所能做出的最后选择。如果路由表没有配置缺省路由,那么当数据包中的目的地址在路由表中没有与之相匹配的路由表项时,数据包就会被丢弃。一般对于末端网络节点而言,缺省路由可以大大简化路由器的配置,减轻管理员的工作负担,提高网络性能。

但如果两条缺省路由时,数据包就会随机选择其中一条路由条目来进行数据转发,对华为路由器而言,会一直使用此条错误的路由条目进行数据转发,可以看出,计算机 B1 不能正常进行数据转发,因为选择的路由条目是不可达的“36.130.254.11”这个 IP 地址,导致数据一直不能转发成功。

笔者使用“undo ip route-static 0.0.0.0 0.0.0.0 36.130.254.11”命令,将不正确的路由条目进行了删除,然后保存配置,重启路由器,B1 发送数据恢复正常,其他计算机给上级发送数据也都恢复正常,故障排除成功。

经验总结

发生故障的原因,是单位新购了一台路由器对该网络的原用路由器进行了置换,原用路由器因使用时间过久,出现了无故重启和以太网接口无故 Shutdown 的现象。新来的同事对缺省路由理解不深,给路由器配置了两条缺省路由,导致网络异常。

当在一台路由器中如果有多条通信信道都可以达到同一目标网络时,那么可以配置多条静态路由来实现负载均衡,也可以采用缺省路由来实现此功能。而当仅有 1 条外连通信信道时,是不能配置多条缺省路由的,这不仅达不到负载均衡的作用,还会导致网络异常。

此外,在完成路由器的配置之后,一定要对网络进行一个全面的测试,以确保网络中的所有用户都可以正常对外连通网络,而不仅仅是一台计算机能通信正常,就以为路由器配置正确。

限速配置引故障

▼ 山东 何钰 李瑞祥

故障现象

近日有同事反映，最近新提速的互联网用户，测试带宽达不到标准。得知这一故障后，我们继续深入了解问题，原来用户办理的是 10M 提 20M 业务，但是测速结果一直不太理想，始终保持在 10M。

故障分析

对该账号的信息进行详细核对，没有发现问题。在机房搭建测试环境，使用故障用户的账号测试能达到 20M，这也印证了该账号是没有问题的，也进一步说明互联网出口也没有拥塞。我们了解到，用户的接入方式是光纤入户，该账号不存在问题，是否故障存在该用户使用的 OLT 上呢？

故障解决

在该 OLT 上搭建测试环境，对故障用户的账号进行测试，也没有发现异常。继续排查该用户的 ONU 配置，在这里我们发现了端倪。ONU 端口的配置如下：

```
interface epon-onu_1/1/2:22
// 进入 ONU
service-port 1 vport 1 user-vlan 2000 to 2999 svlan
2064
// 定义端口的 QINQ 规则
service-port 2 vport 1 user-vlan 1000 to 1999 svlan
1064
```

// 定义端口的 QINQ 规则

```
sla upstream assured 3072 maximum 10240
```

// 定义 ONU 的上行带宽

```
sla downstream maximum 10240
```

// 定义 ONU 的下行带宽

通过查看 ONU 的配置命令，可以看到 ONU 上配置了上下行限速。找到了故障原因后，立即对该命令进行删除：

```
interface epon-onu_1/1/2:22
```

// 进入 ONU

```
no sla upstream
```

// 删除上行限速

```
No sla downstream
```

// 删除下行限速

完成 ONU 端口上下行限速命令的删除后，故障用户的测试带宽能准确地达到 20M，故障得以解决。

经验总结

从得知故障现象，层层缩小故障范围的，将故障定位在了 ONU 端口，配置了上下行限速命令，将该命令删除后故障得以解决。

后期我们得知，该 OLT 开局之初配置时，配置 ONU 的限速命令是操作规范，符合运营商对用户 10M 宽带限速的要求。而在处理上述故障时，没有达到活学活用的目的，最终导致了故障的发生。根据此故障，我们将该品牌的 OLT 进行了逐个筛查，从而杜绝此类事件的发生。

光模块选型不当网不通

福建泉州 王刚 余鑫海 叶伟

故障现象

单位有一台华为 AR2220 路由器，因业务拓展需要，将原有路由器的 Combo 复用接口的电口功能转换成光口功能，加装 1 个 LE2MGSC40DE0 光模块，以连接不足 5 公里之外下属单位的路由器 AR2220 的光模块。加装完成并使用光纤跳线对路由器之间的光模块进行连接，连接完成后开启路由器，两台路由器光模块接口 LINK 指示灯不亮，物理链路不通，数据无法传输。

引起链路无法连通的可能原因

1. 路由器配置不当

华为路由器 Combo 复用接口是光模块接口和路由器的电口 GigabitEthernet 0/0/0 复用，二者只能选其一，如果将此复用接口当电口使用时，其光口功能无法使用。如果将此复用接口当光口使用，则电口功能无法使用，路由器默认此复用接口为电口功能，当路由器未启用光口功能时，即使两端连接了光模块，物理链路也是不通的。

2. 光纤跳线、光模块等存在物理故障或使用不匹配

当光纤跳线或光模块存在物理故障时，会导致物理链路无法连通。当使用的光纤跳线同光模块不匹配时，也会造成物理链路无法连通。

笔者有遇到过光纤跳线完好但光路仍无法连接的故障，其主要原因是光纤跳线使用不当，因光纤跳线的接头截面有平的、有带倾角的、也有圆锥形，如果光纤跳线同光模块接头截面不匹配，物理链路也是无法连通的。

此外，因光模块为单芯双向连通，使用的光模块两端必须为 A-B 型，即一端为 A 型光模块，另一端为 B 型光模块，两端的收发波长需要相互匹配方可（假设 A 型光模块的发送波长为 1310nm，接收波长为 1550nm 时，B 型光模块的接收波长必须是 1310nm，发送波长

为 1550nm，同 A 型光模块刚好收发刚好相反）。

3. 各接口连接不紧密

当光纤跳线同光路的耦合器、光纤跳线同光模块及光模块同路由器连接不紧密时，也会造成物理链路无法连通。

4. 光纤线路断裂和损耗过大

光纤线路在长时间使用过程中，因外部原因极易造成光纤线路弯曲，被挤压，甚至会遇到虫啃鼠咬，导致光纤线路断裂和损耗增加，在这种情况下，链路也无法连通。

5. 光模块同路由器不匹配

不同型号的路由器匹配的光模块型号也不同，中低端的光模块不一定适用于高端路由器，高端光模块也不一定适用于中低端的路由器。此外，路由器加装的光模块一般都需要经过路由器生产厂商认证方可使用。

6. 线路上光衰选择不当或光模块选型不符合实际链路

这种可能性也会有发生，但不常发生。一般有三种情况：第一种情况是当光模块的发送 / 接收功率不足或光纤线路损耗过大时，会造成光模块无法连通。第二种情况是当光模块发送功率过大或光纤线路过短也会导致光模块无法连通。第三种情况比较极端，就是使用 1550nm 波长的接收端可以正常接收信号，而使用 1310nm 波长的接收端却无法接收到信号，原因是 1310nm 波长和 1550nm 波长的衰减值不同，1550nm 波长衰减值一般为 0.25dB/Km，而 1310nm 波长衰减值一般为 0.4dB/Km，1310nm 波长衰减快，而 1550nm 波长衰减慢造成的。

故障排查

1. 确认光模块属性是否匹配路由器

经查询，华为 AR2220 路由器支持 LE2MGSC40DE0 光模块，该模块使用距离为 40Km，速率为 1.25Gbit/s，

所购买的光模块也是经过华为公司认证的光模块，光模块的速率与光接口速率相匹配，光模块同路由器匹配。

2. 查看路由器配置是否正确

查看路由器的 Combo 复用接口设置是否正确。查看命令如下：

```
<Huawei> system-view
[Huawei] interface GigabitEthernet 0/0/0
[Huawei-Gigabit Ethernet0/0/0] display this
```

其显示结果如下：

```
#
Interface Gigabit Ethernet 0/0/0
#
Return
```

从显示结果可以看出，路由器的 GigabitEthernet 0/0/0 仍为电口模式，而不是光口模式，设置错误。

将 GigabitEthernet 0/0/0 设置为光口模式的命令如下：

```
<Huawei> system-view
[Huawei] interface GigabitEthernet 0/0/0
[Huawei-Gigabit Ethernet0/0/0] combo-port fiber
[Huawei-Gigabit Ethernet0/0/0] display this
```

其显示结果如下：

```
#
Interface Gigabit Ethernet 0/0/0
combo-port fiber
#
Return
```

从显示结果可以发现，GigabitEthernet 0/0/0 已经变为光口模式，端口模式设置正确，将两台路由器的 GigabitEthernet 0/0/0 全部设置为光口模式后，路由器之间仍为连通，链路未恢复正常。

3. 检查光纤跳线和光模块

光纤跳线端口截面为平的，使用的为 LC 跳线，同光模块相匹配，更换了几条新的跳线以及连接的耦合器，链路未恢复正常。检查两台路由器的光模块收发工作波长相匹配，其结构类型为 A-B 型，不存在 A-A 型或 B-B 型现象，使用其他新的光模块依次更换路由器两端的光模块，链路未恢复正常。

4. 检查光纤线路

因两台路由器之间的距离不足 5Km，使用激光笔从光纤线路一端发射激光，在另一端可以清晰查看到激光束，证明光纤线路没有断点。后使用一对光纤收发器对线路进行测试，并在光纤收发器两端接入两台计算机，两台计算机之间可以 Ping 通，时延小于 1ms，没有出现掉包现象，证明光纤线路正常。

5. 检查光模块同光纤线路是否匹配

进入路由器用户配置模式，使用 display transceiver verbose 命令查看光模块信息，检查是否有告警，根据告警信息做相应处理，方法如下：

```
<Huawei> display transceiver verbose
```

其显示结果如下：

```
Alarm information: RX power High
```

根据显示结果可以看出，光模块接收到的光信号过高，后在光纤线路中加入光衰减器，光模块接口 LINK 指示灯亮起，故障排除，链路恢复正常。

经验总结

这起故障的原因是因为给华为 AR2220 路由器匹配的光模块选型过高造成的，两台路由器之间的距离不到 5 公里，而光模块的实际通信距离可以达到 40Km（实际达不到 40Km），在光纤链路衰减小的情况下，造成光模块之间无法连通。所以，在正常给路由器或交换机选用光模块时，一定要根据实际光纤的长度来选型，不一定选型越高就越好，要综合考虑光纤链路的实际损耗、日后链路和设备损耗等因素。

在光纤链路正常的情况下，光模块的理论通信距离是实际距离的 1.5-2.5 倍就可以，过高过低都容易造成光模块不能正常工作。

如果误将长距离光模块使用在短距离场景时，则由于光功率过大导致光接口不能 LINK，甚至烧毁光模块接收器，短距离场景下使用长距离光模块时，光模块与光纤之间一定要加入适当光衰，减少光模块发射功率。

当误将短距离光模块使用在长距离场景时，会因为发射功率不足而导致物理链路无法正常通信。

策略路由缺失引发故障

山东 何钰 李瑞祥

策略路由，是一种比基于目标网络更加灵活的路由转发机制。路由器根据策略路由形成的路由图对需要路由的数据包进行处理，路由图则决定了一个数据包的下一跳转发路径。如果策略路由缺失，就会造成数据转发故障，进而影响互联网用户的正常使用。

故障现象

近日，某些大客户专线报修，故障现象是能正常拨号，但是网页不能正常浏览。

故障分析

“能拨号成功但是打不开网页”，第一感觉就是 DNS 出现问题，但是经过对 DNS 一系列检查后均没有发现问题。使用 Ping 命令测试到 BRAS 和路由器的连通性也没有发现问题的。在机房搭建测试环境测试，通过查找资料，得知该大客户专线使用的互联网出口为省公司出口。这里先介绍一下网络的拓扑结构，OLT 直连 BRAS，BRAS 连接两台核心路由器形成双归属，从而实现数据的负载分担。然后两台路由器分别连接省公司出口和第三方出口，使用省公司出口的 IP 地址是在两台路由器上使用策略路由实现的，而使用第三方出口的 IP 地址是在两台路由器上是用默认路由实现的。

刚才提到的这部分大客户专线，使用的是省公司出口，那么需要匹配策略路由才能将数据转发出去。随即排查核心路由器上的策略路由条目，在匹配省公司策略路由的 ACL 条目中，并没有发现这部分大客户专线使

用的 IP 地址。

故障解决

立即在两台路由器上进行 ACL 的添加，具体配置步骤即：

```
ipv4-access-list SHENGGONGSI
// 进入 ACL 列表
rule 33 permit 10.220.224.0 0.0.15.255
// 创建新的 ACL 条目
```

在两台核心路由器上完成 ACL 条目的添加后，ACL 列表就会重新在 route-map 中调用，从而策略路由完成在端口上的应用。配置完这一命令后，我们使用 Trace 命令对路径进行了跟踪，可以准确地看到该大客户专线用户的 IP 地址已经到达省公司，再一次测试网络，可以正常访问 Internet，故障得以解决。

经验总结

该专线正常应该匹配策略路由将数据转发至省公司，由于策略路由 ACL 条目中路由的缺失，导致数据不能正常转发至省公司。该段 IP 地址在核心路由器上会按照默认路由转发至第三方出口，但是第三方出口并没有该网段的路由，所以数据也转发不出去。这才出现文章开头的那一幕，用户能正常拨号，但是打不开网页。

后期该故障的发生，是因为我们进行数据割接和互联网出口扩容时，没有理清使用出口的 IP 地址而造成的。

PoE 供电引发故障

天津 雷远东

PoE (Power Over Ethernet) 供电俗称以太网供电,是指在现有的以太网布线基础架构不做任何改动的前提下,在为一些基于 IP 的终端传输信号的同时,还能为此类设备提供直流供电的技术。POE 供电已成为利用以太网同时传送数据和电功率的最新标准规范,并保持了与现存以太网系统和用户的兼容性。

随着 IP 电话、无线 AP、网络监控等设备被大量引入, POE 供电由于具备技术成熟、维护简单、布线方便等优点得到了广泛应用,给企业信息化建设带来了极大便利。但是不久前,笔者所在单位发生了一起网络故障,最终排查出的故障原因正是由于 POE 供电不当所引起。下面将对该故障及排查过程进行详细介绍。

故障现象

不久前,笔者所在单位进行网络改造,目的是对 Internet 出口架构进行优化,加强 Internet 线路保障水平。主要工作是在原有的联通 Internet 线路之外,额外引入一条移动的 Internet 线路作为备用线路。同时,更新出口互联交换机以及撤除老式防毒墙(原互联交换机及防毒墙已使用 6 年,严重老化)。经过前期准备及紧张的调试后,网络改造工作顺利完成,经过测试, Internet 出口功能和性能都达到了预期,改造后的出口拓扑如图 1 所示。

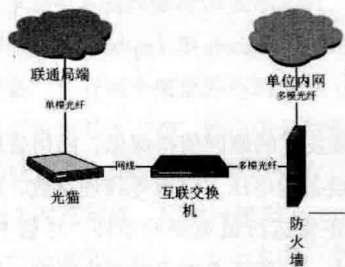


图 1 改造后的 Internet 出口拓扑图

正当大家还沉浸在改造成功的喜悦中,问题出现了:

改造后第二天上午 9:30 左右,联通线路突然中断,笔者赶紧利用 traceroute 命令进行排查,发现内网路由均正常,但是从单位防火墙到运营商局端设备间数据不能正常跳转,说明问题应该出现在防火墙或者局端。登录防火墙检查状态,发现 CPU 利用率、内存、并发连接数等关键指标均正常,但是使用 Ping 命令去测试联通线路局端网关,却无法 Ping 通;而 Ping 移动线路局端网关,却能够正常 Ping 通,这样就排除了防火墙的问题,证明故障肯定出现在防火墙之外的局端。

接着检查了光猫的状态,发现 TX (发送) 口和 RX (接收) 口指示灯时断时续,这与正常时的状态不一致,说明光猫收发数据不正常。重启光猫,线路立即恢复了正常。但是到 11:00 左右,线路又一次中断,现象与之前一模一样,但是这次故障时间很短,大概只持续了 1 分多钟,笔者还没来得及做任何操作,线路已经自行恢复正常了。

故障排查

从故障现象初步分析,联通线路中断的根源很可能是光猫,那么更换光猫后故障应该可以解决。于是联系联通客服人员,要求更换光猫。下午 5:30 下班后,联通人员到达现场,更换了光猫,测试亦未发现任何异常。

第三天早上 8:10 左右,联通线路再次闪断 2 分钟,由此看来,故障并不是由光猫自身导致的。在排除线路、设备等硬件故障后,笔者考虑到了电流、电压的问题。但是经过仪器实际检测,机房电源、UPS 设备以及插线板的电压都非常稳定,而且机房其他设备也没有出现类似问题,所以能够排除机房电源的问题。

为了尽快解决这个问题,我们采用了“最近变更回退”的方法进行排查。由于这次故障是在进行网络改造后出现的,必须分析这次改造所涉及的变更操作,并与改造前的正常状态进行对比,必要时进行回退操作。主

要变更操作有如下三项：

1. 防火墙上新接入一条移动 Internet 线路，设置了若干条源地址路由，供部分服务器使用。
2. 撤掉了位于防火墙和运营商局端的一台老式防毒墙，该防毒墙一直以透明网桥的模式接入。
3. 更新升级了互联交换机。由原来的思科 2960 百兆交换机更换为思科 3560 千兆交换机。

故障分析

下面就按照上述三条变更操作逐步进行分析。

1. 该操作主要是进行了路由变更，属于“软变更”。通过仔细核对防火墙配置文件，发现并无问题，而且故障现象是线路时断时续，如果属于路由设置错误，一般不会出现如此现象，所以能够排除该变更的可能性。

2. 该项操作属于“硬变更”，由于防毒墙属于透明网桥接入，所以撤掉防毒墙的操作并不会影响网络的运行，反而能够减少一个故障点，所以也能够排除可能性。

3. 该项操作属于“硬变更”，前期通过检测，新更换的思科 3560 交换机运行状态正常，能够排除交换机硬件损坏的可能性。由于交换机上采用的是默认配置，所以不会出现由于人为配置错误而导致网络故障的可能。但是由于新旧交换机型号和 IOS 内核版本并不一致，所以不能完全排除交换机自身的原因。

为了确定交换机是否为故障源头，笔者将原来的 2960 交换机重新上线，替换下 3560 交换机。经过两天的测试，联通线路没有出现任何故障，由此看来，故障源头已经确定为交换机，原因肯定是新旧交换机的逻辑属性不一致，从而引发与之互联的光猫状态异常。

笔者仔细对两款交换机的逻辑属性进行了对比，有如下两点属性不同：第一，2960 交换机都是百兆端口，而 3560 交换机都是千兆端口。第二，2960 交换机不支持 POE 端口供电，而 3560 交换机支持 POE 端口供电。

光猫的以太网接口为百兆全双工模式，而 3560 交换机为千兆接口，尽管当前绝大多数网络设备均支持端口速率自适应，但是还是存在端口速率不匹配的可能性。通过 Console 口登录 3560 交换机，进入接口模式，输入“speed 100”和“duplex full”两条命令，将对应接口强制指定为百兆全双工模式。改完后测试两天，线路仍然频繁出现闪断现象，所以排除了端口速率不匹配的因素。

设备供电流程

POE 供电系统是由供电端设备（PSE，Power Sourcing Equipment）和受电端设备（PD，Powered Device）两部分组成；其供电流程如下所示：

1. 检测：一开始，POE 设备在端口输出很小的电压，直到其检测到线缆终端的连接为一个支持 IEEE 802.3af 标准的受电端设备。

2. PD 端设备分类：当检测到受电端设备 PD 之后，POE 设备可能会为 PD 设备进行分类，并且评估此 PD 设备所需的功率损耗。

3. 开始供电：在一个可配置时间（一般小于 15 μs）的启动期内，PSE 设备开始从低电压向 PD 设备供电，直至提供 48V 的直流电源。

4. 为 PD 设备提供稳定可靠的 48V 直流电，满足 PD 设备不高于 15.4W 的功耗。

5. 若 PD 设备从网络上断开时，PSE 就会快速地（一般在 300 ~ 400ms 之内）停止为 PD 设备供电，并重复检测过程以检测线缆的终端是否连接 PD 设备。

故障解决

从上述流程中可以看出，3560 交换机承担 PSE 角色，光猫成为 PD 角色；在 PSE 检测阶段，3560 交换机会持续向光猫输出极小的电压，而由于光猫是利用外接电源供电，不支持 POE 供电，所以这个检测电压可能会对光猫的工作电压带来一定冲击，如果光猫对工作电压的稳定性要求很高，那么检测电压很可能造成光猫运行异常。

为验证结果，笔者登录 3560 交换机，在接口配置模式下，输入“power inline never”命令，强制关闭对应接口的 POE 供电功能。后经过测试观察，联通线路再没有出现异常。

经验总结

这起故障发生的原因值得深思，网络管理人员经常会忽视网络设备的电压、电流等物理参数，殊不知这些参数是设备正常运行最重要的条件。尽管 POE 供电的测试电压极小，一般不会对设备产生影响，但是为了防微杜渐，在实际工作中最好将 POE 和非 POE 设备区分开，以免造成难以排查的故障隐患。

故障现象

最近，一次 UPS 故障引起断电后，重新开启服务器和存储阵列，用 vSphere Client 登录 ESXi 主机后，发现该主机下的虚拟机列表都变成灰色了，无法开机，选中任何一台虚拟机都无法进行任何操作。

故障排查

数据名称	数据	数据类型	数量	单位
名称	名称	字符串类型	2.72	个
值	值	字符串类型	2.72	个

[illegible][illegible]

由此推断, ESXi 无法认出磁盘阵列提供的逻辑盘, 是由于停电导致分区表丢失, ESXi 用作数据存储的分区一般是 VMFS 分区, 即 VMFS 分区表丢失导致磁盘无法被 ESXi 认出, 无法读取虚拟机文件, 引起虚拟机的丢失。

故障解决

首要任务就是修复逻辑盘的 VMFS 分区表，以便 ESXi 能够读取逻辑盘，找到虚拟机文件。

一般情况下，存储标识没有显示的话，通过 vSphere Client 登录主机后，选择主机→配置→存储器，在“数据存储”标签下，用“全部重新扫描”和“添加存储器”来找回没有显示标识的设备和加载新的存储器。但是在 VMFS 分区表丢失的情况下，进行重新扫描没有任何作用，而用“添加存储器”确实可以发现两个磁盘阵列的逻辑盘，但是下一步系统会提示这是全新的存储器，要进行格式化等操作。这可万万不行，虚拟机的文件都在里面，只能另想办法了。

经过查阅资料和研究，决定使用 partedutil 命令来对 VMFS 分区表进行修复。首先用 vSphere Client 登录 VMware ESXi 5.5 主机，进入配置→存储器，查看系统的数据存储和设备，设备名称是待一会要用到的。用 SSH2 登录 VMware ESXi 5.5 主机，使用命令对磁盘进行操作，SSH 服务可以在 vSphere Client 中的配置→安全配置文件里进行开启，在此不累述。在以下我们以修复设备图 2 中的逻辑盘 naa.6b083fe000e6b8a60000038a5712bf49 的分区表信息并使之显示正常的数据储存标识为例，来讲述 VMFS 分区表丢失后的修复过程。

以下操作在用 SSH2 登录主机后操作。

1. 查看存在的磁盘设备及分区

```
ls /vmfs/devices/disks/
```

该命令主要是查看现有磁盘的分区信息（如图 4 所示），我们只要看前面一列的磁盘名称即可，后面有冒号 1，说明这是该磁盘的第一个分区，依次类推。可以看出 naa.6b083fe000e6b8a60000038a5712bf49 磁盘下没有分区，其他磁盘下都有一个或多个分区，接下来就要修复该磁盘的分区表，当然我们得事先知道在坏掉以前它是几个分区的，此处我们的逻辑磁盘在分区表坏掉前都是一个分区的（在进行截图时，名称尾号为“79”和“3d”的逻辑盘的分区表已经用此文中的方法修复，因此它们下面都有分区信息）。



图 4 查看所有磁盘的分区信息以及具体某个盘的分区表

2. 用 partedutil 查看某个磁盘上的分区表

确认具体某个逻辑盘具体的分区表的体信息，命令：

```
partedutil getptbl "/vmfs/devices/disks/naa.6b083fe000e6b53c0000025b54a8d579"
```

除了逻辑盘的名称 naa.6b083fe000e6b53c0000025b54a8d579，其他都是固定格式，此命令可以分别查看有分区信息的逻辑盘和分区表丢失的逻辑盘，如图 4 中：

gpt 代表分区格式。

4348570 表示磁盘的柱面数。

255 表示磁头数。

63 表示每磁道扇区数。

69859790554 总扇区数。

“1 2048 69859790520 AA31E02A400F11DB959000 0C2911D1B8 vmfs 0”代表了一条分区表信息，“1”表示第一个分区，“2048”表示起始扇区，“69859790520”表示结束扇区，“AA31E02A400F11DB9590000C2911D1B8 vmfs 0”表示这是 VMware 的数据存储分区，VMFS 分区，“0”是分区属性（一般都是 0），这些是固定格式。

从图 4 可以看出，naa.6b083fe000e6b8a60000038a5712bf49 这个逻辑盘没有分区表了，下面就来修复它的分区表。

3. 用 partedutil 取得磁盘可用的扇区数

```
partedutil getUsableSectors /vmfs/devices/disks/naa.6b083fe000e6b8a60000038a5712bf49
```

因为一个磁盘在 ESXi 中是从 2048 扇区开始使用的，还要去掉 VMFS 分区占用的头部 34 个分区，所以还是用这条命令获取一下可用的扇区数比较合理。注意，这条命令中的参数 getUsableSectors 严格区分大小写。此命令执行后得到数据“34 20971486”，代表该磁盘可用的扇区到“20971486”，这个数据稍后的命令参数中要用到。

4. 重建 VMFS 分区表

得到了磁盘名称，磁盘可用的扇区数，就可以用命令 partedutil 来重建 VMFS 分区表了。本例中，磁盘名称为 naa.6b083fe000e6b8a60000038a5712bf49，最大可用扇区“20971486”，整个逻辑盘只有 1 个分区，其他参数都是固定的。

命令为：

```
partedutil setptbl "/vmfs/devices/disks/naa.6b083fe000e6b8a60000038a5712bf49" gpt "1 2048 20971486 AA31E02A400F11DB9590000C2911D1B8 0"
```

执行后出现提示：

```
gpt
0 0 0 0
1 2048 20971486 AA31E02A400F11DB9590000C291
1D1B8 0
```

表示在这个逻辑盘上的 VMFS 分区建立好了。

至此，磁盘丢失的分区表已经修复。回到 vSphere Client，在图 1 界面进行“全部重新扫描”应该会出现修复回来的数据储存标识，只要再把该存储标识进行“挂载”即可正常使用了。进行“浏览数据存储”，看到数据文件都在。利用同样的方法，修复了其他两个逻辑盘，每个设备对应的数据存储标识都正常显示了（如图 5 所示），丢失的虚拟机又回来了，正常开机，数据完好。



图 5 修复后每个设备对应数据存储标识都正常显示了

经验总结

分区虽然修复了，虚拟机也找回来了，但还是心有余悸，有两点体会特别深刻。

1. 中心机房的设备与环境同样重要。不能光顾着更新服务器、交换机等设备，而忽略 UPS、空调等环境设备，突然的断电，对服务器、磁盘阵列损伤极大，轻者分区丢失，重者直接硬件损坏。

2. 不断学习，不断进步。对服务器虚拟化可以提升资源利用率、减少能耗、减少物理服务器的数量，但是它有时又不像实际服务器那样看得见摸得到，作为使用者我们应该对虚拟机系统有更深入的了解，以便出现问题时能及时找到解决方案。以下是 partedutil 命令的官方说明，对该命令想进一步了解可以参考。

<https://kb.vmware.com/selfservice/microsites/search.do?cmd=displayKC&externalId=2076191>

链路层协议为何报错

湖北 张亚舟

最近公司进行楼层交换机更新改造工程，把楼层的 11 台中低端交换机 Guidway S3928TP-SI 更换为 H3C S5110-28P-SI 交换机。在改造完成后，发现有一台新交换机设备 SW1 无法进行网络管理，但该设备上连接的客户端网络通信正常。

网络结构

公司局域网由两台核心交换机 CW1、CW2 和若干接入层交换机 SW1、SW2 等组成，其中 CW1、CW2 为 H3C S7506E，SW1、SW2 为新更换的 H3C S5110-28P-SI，SW1、SW2 分别通过两条光纤线连接到核心交换机 CW1 和 CW2，实现冗余备份，网络拓扑图如图 1 所示。

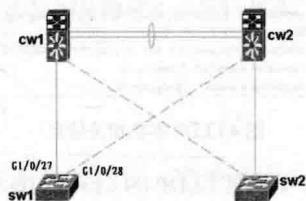


图 1 网络拓扑结构

故障解决

1. 通过 Console 控制口登录 SW1 交换机进行检查，发现配置无误，查看 SW1 交换机日志信息，显示如图 2 所示。

```
%Jan 23 03:01:07:586 2016 SW1 LLDP/5/LLDP_CREATE_NEIGHBOR: New
neighbor created on Port GigabitEthernet1/0/20 (IfIndex 18952192), Chassis ID is
3897-d645-6986, Port ID is GigabitEthernet1/0/15.

%Jan 23 03:27:14:843 2016 SW1 LLDP/6/LLDP_NEIGHBOR_AGE_OUT: Neighbor
aged out on Port GigabitEthernet1/0/20 (IfIndex 18952192), Chassis ID is
3897-d645-6986, Port ID is GigabitEthernet1/0/15.
```

图 2 SW1 交换机日志信息

该日志信息是说，SW1 交换机 20 号端口与 LLDP 的 Chassis ID 为 3897-d645-6986 的交换机 15 号端口互为 LLDP 邻居关系。

2. 经查询，该系列交换机配套文档资料和 LLDP 相关文档，没有发现解决办法，只能从日志信息入手。

3. 查看 SW1 交换机 20 号接口信息，没有发现异常，再看 SW1 和 CW1、CW2 相互之间连接的接口信息，以及 CW1 和 CW2 核心交换机的日志信息，均没有发现异常。

4. 使用 `dis stp brief` 命令查看 SW1 交换机线路冗余情况，显示如图 3 所示，发现 STP ROOT 选举不对，变成了办公室 1 里的 PC 电脑相连接的 GigabitEthernet1/0/20，而不是 SW1 和 CW1 或 CW2 相连接的 GigabitEthernet1/0/27 或是 GigabitEthernet1/0/28。再次检查 SW1、CW1 和 CW2 上的 STP 配置信息，确认配置正确无误。

AISTID	Port	Role	STP State	Protection
0	GigabitEthernet1/0/15	DESI	FORWARDING	NONE
0	GigabitEthernet1/0/20	ROOT	FORWARDING	NONE
0	GigabitEthernet1/0/27	ALTE	DISCARDING	NONE
0	GigabitEthernet1/0/28	ALTE	DISCARDING	NONE

图 3 SW1 交换机线路冗余情况

5. 通过命令 `dis lldp local-information` 查看 LLDP 本机相关信息，显示如图 4 所示。

```
Global LLDP local-information:
Chassis ID       : 3897-d645-3926
System name      : SW1
System description : H3C Switch S5110-28P-SI Software Version 5.20.99,
Release 1106
Copyright(c)2004-2015 Hangzhou H3C Tech. Co., Ltd. All rights reserved.
System capabilities supported : Bridge,Router
System capabilities enabled   : Bridge,Router
```

图 4 LLDP 本机相关信息

发现 SW1 交换机 LLDP 的 Chassis ID 为 3897-d645-

3926，而 SW1 交换机日志信息上显示 Chassis ID 为 3897-d645-6986 的交换机又是哪台交换机呢？

6. 通过查看每个楼层交换机上的 LLDP 相关信息，发现 SW2 交换机 LLDP 的 Chassis ID 为 3897-d645-6986。

再查看 SW2 交换机上的 15 号接口，发现是连接办公室 2 里的 PC 客户端。

7. 经查看，办公室 1 和办公室 2 互为隔壁房间，并且所属同一个网段，办公室 1 和办公室 2 均使用普通交换机连接楼层交换机 SW1 和 SW2，现场对这两台普通交换机上连接的网线摸查发现，有一根网线同时连接着两个普通交换机，从而形成了一个口字型连接结构，该连接结构图如图 5 所示。

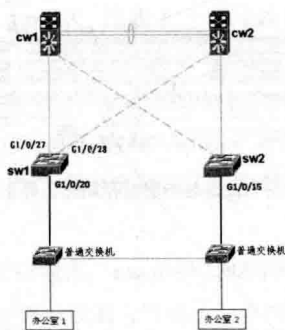


图 5 口字型连接结构

该连接结构是不对的，会造成 SW1 和 SW2 交换机上连接的所有客户端都无法正常通信。拔掉连接两个普通交换机之间的错误网线，一切恢复正常，故障圆满解决。

经验总结

对于发生的网络故障，原因可能是不曾想到或是不该发生的，我们除了查找相关资料，顺藤摸瓜外，还要排查所有相关设备及其线缆。

◆ 精确定位“软故障”源头

▼ 天津 雷远东

突发性的网络故障往往令网络管理人员措手不及，需要在最短的时间内解决故障，恢复业务运转，这也是网络管理人员的价值所在。以往的网络故障很多都是由硬件故障引起的，因此找到故障设备进行更换即可，我们称之为“硬故障”。这种故障解决相对简单，通过对各类网络设备的状态监控即可进行故障定位。

随着硬件工艺水平的提高及容灾技术的发展，发生“硬故障”的概率越来越低。但是由于病毒、木马、ARP 攻击、用户误操作等一系列原因导致的网络故障比例大幅增加，我们称之为“软故障”。解决软故障比解决硬故障更加困难，如果没有丰富的网络维护经验，仅凭网络设备状态监控系统，是很难定位软故障源头的。如果定位不了故障源头，一方面难以解决故障，另一方面也无法向上级领导提供准确的故障报告及相关建议，难以彻底杜绝此类网络故障的发生。所以，解决软故障的能力很大程度上反映了网络管理人员的水平。

笔者所在单位不久前发生过一起网络故障，这次故障牵涉范围很广，对业务的影响也比较大。但是，笔者最终在较短时间内找到了故障源头，及时解决了问题。同时，也提交了详细的故障报。下面将对该起网络故障进行详细介绍。

背景及故障现象

笔者所在单位是在 CBD 大楼办公，各个业务及职能部门分布在不同的楼层，中心机房设置在 5 楼，每个楼层会有一个网络设备间用于放置接入交换机及相关配线架，然后通过综合布线工程将各个楼层办公室的办公电脑接入网络。每层网络设备间的接入交换机与汇聚交换机通过光纤互联，汇聚交换机与核心交换机也通过光纤互联，这是一个典型的“核心-汇聚-接入”的三层网络架构。局域网内服务器 IP 通过静态方式分配，用户电脑的 IP 则是由一台 Windows Server 2003 DHCP 服

务器自动分配。每个楼层都是一个独立的网段，通过 VLAN 技术进行划分，交换机品牌全部为思科。

某工作日上午 8:10 左右，还没有到上班时间，笔者接到用户反映：6 楼业务部门两台电脑无法上网。由于其他楼层的用户上网均无异常，当时笔者以为是病毒或者电脑自身问题所导致，就联系了维护电脑终端的同事前去处理。10 分钟后，同事打来电话，说故障现象很奇怪，那两台故障电脑都进行了重启，一台恢复正常，另一台还是不能上网，而且后续开机的电脑，也是一部分正常，另一部分不能上网。由于马上就要到 8:30 上班时间，如果拖延时间太长，恐怕会影响业务，引起用户不满。

笔者立即亲自赶赴现场，在排除了硬件、病毒及网络后台相关的问题之后，发现故障主机通过 DHCP 获得的 IP 都是 192.168.1.0/24 网段的地址，但是单位 DHCP 服务器统一分配的 IP 均是 172.19.0.0/16 网段的地址，而且分配的网关、DNS 等其他参数也都不正确。如果为故障主机静态指定一个正常 IP，则该主机的网络通信恢复正常。但是故障主机数量太多，不可能挨个手动指定 IP。而且，故障源头没有找到，后续肯定还会出现问题，所以必须尽快找到故障源头并加以解决。

故障分析

故障现象初步分析，用户无法上网的原因就是 DHCP 分配地址错误，但是之前已经排查过单位的 DHCP 服务器，证明其运行正常。考虑到故障仅仅发生在 6 楼业务部门这一个网段，这只能有一个解释，就是该网段内出现了另外一台 DHCP 服务器。用户主机在发出 DHCP 广播请求时，两台 DHCP 服务器均会收到请求包并给出响应，然后将相应的 DHCP 配置下发给对应的主机，这时就会发生冲突，哪个响应包先到达主机，主机就会“采纳”哪台 DHCP 服务器下发的配置，就会出现上述同一网段 IP 地址不一致的现象。

如果主机获得的不是单位 DHCP 服务器下发的配置,那么肯定无法上网。由于单位最近并无访客接入内网,所以能够排除恶意攻击的可能,最有可能就是用户无意的误操作所导致的。只有找出这台冲突的 DHCP 服务器,才能彻底解决问题。

看着故障主机 DHCP 分配的 192.168.1.0/24 网段的 IP,笔者突然想起前期给各部门部署过一些 TP-Link 无线路由器,这些无线路由器内部分配的 IP 就是 192.168.1.0/24 这个网段,但是当初部署时,从楼层交换机出来的主线接入的都是无线路由器的 WAN 口,这两个网段应该逻辑上已完全隔离,即使无线路由器上启用 DHCP 服务,也不会影响到 172.19.0.0/16 网段的主机。除非有人将 WAN 口的主线接到 LAN 口上,并且没有关闭无线路由器自带的 DHCP 服务,这种情况下,无线路由器也会为局域网内其他主机提供 DHCP 服务,造成主机 DHCP 配置混乱,无法正常上网。

故障解决

通过分析得出故障的原因后,下一步就必须找到“惹事”的无线路由器。由于 6 楼业务部门部署无线路由器范围大,且数量较多,每个设备的物理位置也不能确定,挨个排查不现实,只能通过后台数据来进行分析,最终定位目标无线路由器。笔者所采用的步骤如下。

1. 分析单位 DHCP 服务器 IP 分配数据,定位该无线路由器所接入的交换机端口。如果主线接入了无线路由器的 LAN 口,并且接入该无线路由器的终端是从单位 DHCP 服务器获取的 IP,那么主线对应的交换机端口很可能对应多台无线终端,只要找到端口和终端数是“一对多”的关系,那么该交换机端口接入的很可能就是目标无线路由器。由于单位的 DHCP 服务器上记录了当前的终端接入信息,可以通过主机名称来区别是否为手机终端(如图 1)。

172.19.34.24	android	2016-4-29 8:30:06	DHCP	192.168.1.100
172.19.34.25	android	2016-4-29 8:30:06	DHCP	192.168.1.101
172.19.34.26	android	2016-4-29 8:30:06	DHCP	192.168.1.102
172.19.34.27	android	2016-4-29 8:30:06	DHCP	192.168.1.103
172.19.34.28	android	2016-4-29 8:30:06	DHCP	192.168.1.104

图 1 手机终端 DHCP 记录

从图 1 可以看出,主机名中含有“android”字符的记录应该为 android 手机终端,这种命名方式是 android 系统所特有的。下面再通过交换机上的 ARP 表和 MAC 地址转发表来确定这几个手机终端是否都接入同一个交换机端口。由于 DHCP 服务器上已经记录了手机终端的

MAC 地址,所以可以通过“show mac-address address XXXX.XXXX.XXXX”和“show cdp neighbor”命令最终获取手机终端的接入端口,结果如图 2 和图 3 所示。

Tosco-05-08sh mac-add add fcdh.b3c2.403b			
Mac Address Table			
Vlan	Mac Address	Type	Ports
53	fcdh.b3c2.403b	DYNAMIC	Gi0/25
Total Mac Addresses for this criterion: 1			

图 2 接入端口示意图 1

Tosco-05-08sh mac-add add a086.c63e.c829			
Mac Address Table			
Vlan	Mac Address	Type	Ports
53	a086.c63e.c829	DYNAMIC	Gi0/25
Total Mac Addresses for this criterion: 1			

图 3 接入端口示意图 2

从图 2 和图 3 可知,这两个手机终端均接入了同一台交换机的 Gi0/25 口,可以确定从该交换机 Gi0/25 口接入的是目标无线路由器。

2. 定位该无线路由器的物理位置。通过步骤(1)找到目标无线路由器所接入的端口后,我们就可以着手进行处理。为了尽快恢复局域网的正常并找到目标无线路由器的物理位置,笔者在交换机对应端口上使用了“shutdown”命令,将该端口关闭,然后通知故障用户重新启动电脑,果不其然,所有主机立即恢复正常。

过了几分钟后,客服人员打来电话,说 6 楼某业务科室反映手机连接无线路由器无法上网,经过现场检查,该科室无线局域网主线果然是接在 LAN 口上,经核实,系昨天一位同事将笔记本带来公司,但是该笔记本无线网卡是坏的,只能通过有线网络上网,于是顺手将无线路由器上的 WAN 口主线拔下来临时接在笔记本上使用,用完后就随意插到了 LAN 口上,由于无线路由器的 DHCP 功能并没有关闭,结果就导致了今天的网络故障。

至此,此次网络故障的源头已经找到。笔者将主线接回 WAN 口,并将交换机端口重新开启,经过测试,网络恢复正常。

经验总结

这次网络故障属于典型的由于用户误操作而引发的“软故障”。由于故障源头在较短时间内找到,没有严重影响业务,在提交了故障说明后,领导并没有追责。但是从这次故障可以看出,一个合格的网络管理人员必须能在较短时间内以清晰的思路去追溯故障源头,特别是

能够充分利用网络后台相关数据进行深度关联分析，进而解决问题。

随着虚拟化、云计算、无线网络等先进技术在企业

内的推广使用，传统网络架构已经发生了深度变革，这种变化将会引发更多“不可思议”的网络问题，网络管理人员必须要有充足的准备去迎接挑战。

链路聚合解决网络瓶颈

四川成都 朱鑫海

笔者单位的安防监控系统共有视频监控点 1600 余个，采用海康 720P 高清网络摄像机，配有海康安防集成平台服务器 1 台，流媒体服务器 9 台，采取两级存储方式，前端存储采用数 10 台 32 路 NVR（高清网络硬盘录像机），中心备份存储采用 8 台网络存储服务器，每台配 16×2TB 企业级硬盘，安防网络核心交换机是 H3C LS-7508E，存储服务器和流媒体服务器接入交换机是 H3C LS-5800 交换机，前端接入交换机是 H3C LS-5120。这套安防监控系统的运行，极大地提高了我单位安全防范能力。网络结构如图 1 所示。

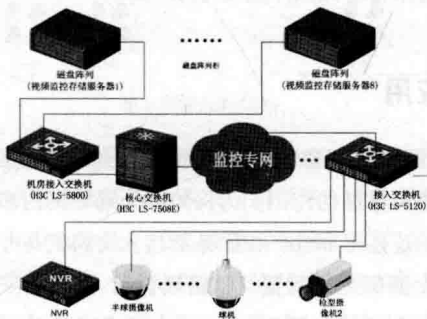


图 1 监控专网及存储服务器组拓扑图

故障现象

一天，某部门经理反映视频监控故障：在回放监控录像时，视频图像卡顿现象（时间断点）较多，比如回放录像播放到 10 时 30 分 10 秒时，突然一下就跳到 10 时 30 分 50 秒去了，提取的录像无法正常使用。检查发现，中心机房备份存储服务器中的录像存在此现象，前端 NVR（高清网络硬盘录像机）的录像则无此现象，即告知该部门经理提取前端 NVR 设备录像文件使用。

故障排查

虽然需要的录像文件拿到了，但存储服务器录像卡顿现象仍然存在，如不及时处置必有后患。随即对 8 台网络存储服务器进行排查，发现最初施工单位技术人员在配置分配存储备份时，把 400 余路监控视频录像加进了第一台网络存储服务器中，而另外 7 台有的只有几十路，有的甚至一路也没有，存储分配极不均衡。

通过向设备厂家咨询了解，每台网络存储服务器所存储的高清监控录像建议不超过 180 路，可见第一台存储设备明显超负荷运行。笔者随即对 8 台网络存储服务器进行了重新规划，把重点部位、重点区域的监控点，配置为两级存储，每台网络存储服务器存储约 132 路监控录像。重新规划配置完成后，通过数天观察，发现故障依旧。又按照厂方指导，对流媒体服务器、平台软件进行检查，并升级存储服务器软件，再观察，故障依然存在。

经反复排查，发现存储服务器网络不稳定。检查服务器接入交换机（H3C LS-5800，48 个 10/100/1000Base-T 端口，4 个 1/10G SFP），其中 1 个万兆光口通过单模光纤与核心交换机相连，但核心交换机上与之连接的端口却是千兆光口。再反复检查核心交换机（H3C LS-7508E），没有找到一个万兆端口可供连接。于是初步断定故障原因是核心交换机至服务器区接入交换机之间的网络瓶颈，造成网络存储服务器录像出现卡顿现象。

但疑问又来了，上千路的监控录像需要传入中心机房进行储存，为什么服务器接入交换机有万兆光口，而核心交换机上却没有万兆光口。经过仔细查看招标文件与合同书，中标集成商所提供设备符合招标要求，核

心交换机无万兆光口属设计遗漏。

解决方案

问题找到了，正常的解决方法就是购买一块万兆业务板卡加在核心交换机上，但经过了解市场，H3C 交换机的万兆业务板卡动辄数万元，为了减轻单位资金压力，决定对交换机配置“链路聚合（link-aggregation）”方式，以实现带宽扩展。

链路聚合，是指将交换机的数条物理链路端口通过配置命令使其聚合在一起，形成聚合组，作为一条逻辑链路来使用，可以实现网络负荷在聚合组各成员端口之间分担，增加带宽，同时，聚合组各成员端口之间又彼此动态备份，提高了网络连接可靠性。

利用“链路聚合”可增加带宽的作用，在核心交换机和服务器接入交换机上选取数千兆端口配置为“链路聚合”组，达到提高网络带宽，消除网络瓶颈目的。按 8 台存储服务器，每台 132 路视频，每路视频最高码率 4096Kbps 计算，则总带宽为： $8 \times 132 \times 4096\text{Kbps} / 1024 = 4224\text{Mbps}$ 。假设选取六个千兆端口配置为聚合组，则 $4224\text{Mbps} / 6000\text{Mbps} = 0.704$ ，满足带宽需求，且有一定冗余。

配置交换机

在两台交换机上分别配置“链路聚合”的方法和参考命令如下（此命令华为交换机类似，但不适用锐捷、思科等交换机）。

1. 进入全局配置模式，并创建聚合组。

```
<S7508E-X>system-view
```

```
[S7508E-X]interface Bridge-Aggregation 1
```

2. 配置聚合组类型。

```
[S7508E-X-Bridge-Aggregation1]port link-type trunk
```

```
[S7508E-X-Bridge-Aggregation1]port trunk permit
```

```
vlan all
```

3. 配置加入聚合组的交换机端口类型（应与聚合组相同）。

```
[S7508E-X]interface GigabitEthernet3/0/1
```

```
[S7508E-X-GigabitEthernet3/0/1]port link-type trunk
```

```
[S7508E-X-GigabitEthernet3/0/1]port trunk permit  
vlan all
```

4. 将端口添加进聚合组中。

```
[S7508E-X-GigabitEthernet3/0/1]port link-aggregation  
group1
```

5. 其他 5 个端口按相同方法加入聚合组。

6. 通过命令 `display link-aggregation verbose` 查看端口是否变成 select，以验证聚合是否成功。

7. 按以上方法配置第二台交换机。

配置时需注意每个端口的类型、运行模式、速率等需一致，并且未作 MAC 绑定、安全配置等，否则会聚合失败。

配置完成后，在两台交换机之间使用 6 根六类网线相连接，并断开之前的光纤连接。再次对网络存储服务器进行测试，网络延时降低，网络带宽明显改善，网络瓶颈消除。理论上网络带宽由原来的 1000Mbps 增加为 $6 \times 1000\text{Mbps}$ ，通过一周时间运行观察后，中心备份存储服务器录像卡顿故障完全排除。

扩展应用

“链路聚合”除了提高带宽外，还具有链路互备，提高网络可靠性的作用。为保障办公局域网内多台应用服务器的连接可靠性，在服务器接入交换机与办公局域网核心交换机之间配置“链路聚合”，由原来一条物理链路，改为两条物理链路通过“链路聚合”连接，一方面提高了应用服务器接入网络的可靠性，又增加了网络带宽。



用时钟反转调试路由

福建泉州 李贵华 荣世辉 郑洪飞

网络结构

笔者单位因业务发展,需要新部署一套网络。由于下级单位条件限制,加上该套网络的特殊性,不能使用互联网 VPN 模式进行互联。因此,租用电信 2M 链路通过调制解调来组建该网络,在两端分别使用新购置的华为 AR1220-S 路由器、华为 2SA 同异步接口卡和 ASM40 基带猫,路由器之间封装 PPP 协议,网络拓扑结构如图 1 所示。

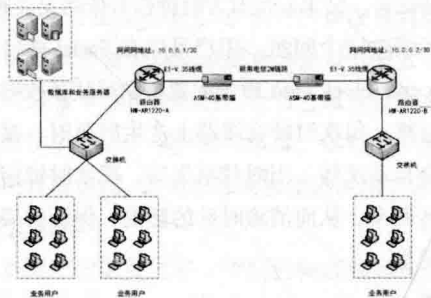


图 1 网络拓扑结构

由于单位部分网络一直使用 ASM40 基带猫进行互联,笔者感觉这次部署就算采用新设备,也应该没有什么问题,并没有拿相关设备做调试实验。直接协调电信调通 2M 物理链路,通知下级单位网络管理员按照网络拓扑规划配置好路由器参数接入网络,结果路由器和基带猫显示均正常,但两点之间的网络始终不能互通。

路由调试过程

再次检查本端路由器和基带猫,两个设备状态灯均显示正常,基带猫之间的 2M 链路也能正常通联。联系下级单位的网络管理员,他们反映路由器和基带猫均显示正常,应该判断是路由器的配置错误造成的网络故障。

于是登录路由器,查看路由器连接端口状态,具体信息如图 2 所示。

```
[HW-AR1220-A]display interface serial 2/0/0
Serial2/0/0 current state : UP
Line protocol current state : DOWN
Description:HWAR1220-A, AR Series, Serial2/0/0 Interface
Route Port, The Maximum Transmit Unit is 1500, Hold timer is 10(sec)
Internet Address is 20.0.0.2/24
Link layer protocol is PPP
LCP stopped
Last physical up time : 2016-01-15 17:08:02
Last physical down time : 2016-01-15 17:08:02
Current system time: 2016-01-15 17:10:35
Physical layer is synchronous, Virtualbaudrate is 64000 bps
Interface is DCE, Cable type is V35, Clock mode is DCECLK
Last 300 seconds input rate 0 bytes/sec 0 bits/sec 0 packets/sec
Last 300 seconds output rate 2 bytes/sec 16 bits/sec 0 packets/sec

Input: 0 packets, 0 bytes
Broadcast: 0, Multicast: 0
Errors: 20, Runts: 0
Giants: 0, CRC: 0

Alignments: 0, Overruns: 0
Dribbles: 0, Aborts: 20
No Buffers: 0, Frame Error: 0

Output: 61 packets, 1406 bytes
Total Error: 0, Overruns: 0
Collisions: 0, Deferred: 0

DCD=UP DTR=UP DSR=UP RTS=UP CTS=UP
Input bandwidth utilization : 0%
Output bandwidth utilization : 0.06%
```

图 2 串口 2/0/0 接口信息

[HW-AR1220-A]display interface serial 2/0/0

通过查看该端口得知,该端口的物理链路为 UP,链路协议 DOWN,PPP 协议协商为 stopped 状态。让下级单位管理员在 ASM40 基带猫前链路远环,发现本段路由器不收远环,具体状态为:物理链路为 UP,链路协议还是 DOWN,通过 2M 线路测试仪测试发现单位之间的物理链路是正常的。

仔细研究端口状态,发现路由器 serial 2/0/0 工作在同步工作方式,而连接基带猫需配置在异步工作方式。

配置端口为异步工作方式

在实际应用过程中,一般来讲路由器均为 DTE 模式,时钟授时是由链路来负责的。于是将上下两级路由器的端口工作方式都改为异步工作方式。需要注意的是,Serial 接口在切换工作方式时,为了保证 Serial 接口流量统计正确,还需要清除接口下的统计信息。具体配置命令如下:

```
[HW-AR1220-A] interface serial 2/0/0
// 配置 Serial2/0/0 接口为异步工作方式
[HW-AR1220-A-Serial2/0/0] physical-mode async
// 清除接口下的统计信息
```


[HW-AR1220-A] reset counters interface serial2/0/0

这里需要说明一下, Serial 接口有两种工作方式: 同步方式和异步方式。当将 Serial 接口作为 DDN(Defense Data Service) 专线或者使用 Serial 接口接入终端时, 工作在同步方式; 当将 Serial 接口作为异步专线或使用 Serial 接口进行 Modem 拨号、数据备份和接入终端时, 工作在异步方式。当设备的 Serial 接口配置为同步方式或异步方式时, 其对端设备的 Serial 接口必须配置为相同的方式。目前像华为 AR1220 等同等级别的路由器缺省情况下, Serial 接口工作在 DCE 工作模式。

配置时钟反转

将路由器 Serial2/0/0 接口配置成异步工作方式后, 将接口 shutdown 后重新启动, 网络仍然不能通联, 看来不只是这个问题。于是笔者打开路由器的 Debug 调试信息:

<HW-AR1220-A>debugging ppp lcp packet interface Serial 2/0/0

运行结果如图 3 所示, 发现 PPP 协议未成功协商。

```
<HW-AR1220-A>debugging ppp lcp packet interface Serial 2/0/0
<HW-AR1220-A>
Jan 15 2016 17:15:32.886.1400:00 up PPP/7/debug2:
PPP Packet:
Serial2/0/0 Output LCP(c021) Pkt, Len 18
State request, code Config(01), id 33, len 14
MRU(1), len 4, val 05dc
MagicNumber(5), len 6, val 7b79b2f6
<HW-AR1220-A>
Jan 15 2016 17:15:35.886.1400:00 up PPP/7/debug2:
PPP Packet:
Serial2/0/0 Output LCP(c021) Pkt, Len 18
State request, code Config(01), id 34, len 14
MRU(1), len 4, val 05dc
MagicNumber(5), len 6, val 2cb45cde
```

图 3 Debug 调试信息

通过查阅有关资料后发现, 如果 DTE 端接收报文有错误, 特别是报文数与字节数没有整数倍对应关系的时候 (如 100 个 packets, 105 Bytes), 此时在接口下配置 invert receive-clock, 将接收时钟反转。如果 DTE 端接收报文没有错误, 但是 DCE 端接收报文还是有错误, 则在接口下配置 invert transmit-clock, 将发送时钟反转。如果将 invert receive-clock 和 invert transmit-clock 都配置后接收报文错误仍然有增长, 则可能与时钟反转无关。

通过图 4 不难发现, 该接口接收报文有错, 于是在该接口下配置时钟反转。具体配置如下:

```
Input: 0 packets, 0 bytes
Broadcast: 0, Multicast: 0
Errors: 20, Runts: 0
Giants: 0, CRC: 0

Alignments: 0, Overruns: 0
Dribbles: 0, Aborts: 20
No Buffers: 0, Frame Error: 0

Output: 61 packets, 1406 bytes
Total Error: 0, Overruns: 0
Collisions: 0, Deferred: 0

DCD=UP DTR=UP DSR=UP RTS=UP CTS=UP
Input bandwidth utilization : 0%
Output bandwidth utilization : 0.06%
```

图 4 DTE 接收报文详细信息

[HW-AR1220-A] interface serial 2/0/0

// 配置反转同步方式下 Serial 接口的接收时钟信号。

[HW-AR1220-A -Serial2/0/0] invert receive-clock

在 A、B 两路由器配置完以上命令后, 将互联接口 shutdown 后重新启动, 发现两台路由器网间网能互通, 路由故障排除。

从厂商技术支持处了解到, 在某些特殊情况下, 时钟在线路上会产生时延, 导致两端设备失步或报文被大量丢弃, 这时可以将设备的异步串口的发送或接收时钟信号反转, 以消除时延的影响。

这里大家还要注意一条命令: invert receive-clock auto, 该命令用来自动反转异步方式下 Serial 接口的接收时钟信号。在线路信号受到频繁干扰等特殊情况下, 时钟在线路上可能会不定时地产生时延, 普通的反转设备 Serial 接口的接收时钟信号 (通过 invert receive-clock 命令配置) 只能反转一次接收时钟信号, 对后面的时延无法继续反转; 而且时延消失的时候, 接收时钟信号也不会自动反转回来, 结果对接双方时钟信号依然无法同步。

为了解决这个问题, 用户可以在 Serial 接口上执行 invert receive-clock auto 命令配置自动反转接收时钟信号功能, 这样, 每次时钟在线路上产生时延时, 接收时钟信号就会自动反转; 当时延消失后, 接收时钟信号还会自动反转回来, 从而消除时延的影响, 保证对接双方时钟信号同步。

当然, invert receive-clock auto 命令不能与 invert receive-clock 命令在同一接口下配置。

经验总结

此次部署网络出现故障, 原因就是采用新设备而没有做相关的通联测试, 加上对路由器异步工作原理掌握不清楚, 导致了一次路由器配置的自摆乌龙。其实在异步工作模式下, 如时钟选择、时钟反转、同异步模式选择、波特率设置等因素都会影响到协议协商成功与否。



用事件查看器查故障

▼ 云南 唐国军 宋云涛

微软在以 Windows NT 为内核的操作系统中都集成有事件查看器，它是 Microsoft Windows 操作系统工具。

Windows 事件查看器的作用

Windows 事件查看器的作用主要有四个：查看信息、搜索事件、存放日志和解决问题。

1. 查看信息

选中事件查看器左边的树形结构图中的日志类型（应用程序、安全性或系统），在右侧的详细资料窗格中将会显示出系统中该类别的全部日志，双击需要查看的日志，便可以查看其详细信息。在日志属性窗口中可以看到事件发生的日志、事件的发生源、事件的种类、ID 以及事件的详细描述。这对解决所发生的故障非常有用。

2. 搜索事件

如果系统中的事件过多，我们将很难找到真正导致故障发生的事件，可以使用事件“事件查看器”中的“刷选”功能找到我们想找的日志，方法介绍如下。

选中左边的树形结构图中日志类型，右击“查看”，并选择“刷选”，日志刷选器将会启动。选择所要查找的事件类型，比如“错误”，以及相关的事件来源和类别等，并单击“确定”。事件查看器会执行查找，并只显示符合这些条件的事件。

3. 存放日志

系统日志中存放了 Windows 操作系统产生的信息、警告或错误。通过查看这些信息、警告或错误，用户不但可以了解到某项功能配置或运行的情况，或者直接可以知道其产生错误的原因。而安全日志中存放了审核事件是否成功的信息，通过这些信息，我们可以了解这些安全审核是否成功。

同样的，应用程序日志中存放应用程序产生的信息、警告或错误。通过这些信息，我们可以了解哪些应用程序成功，产生了哪些错误或潜在错误。

4. 解决问题

查找导致系统问题的事件后，需要找到解决问题的方法。其中的很多问题我们可以通过微软在线技术支持知识库及 Eventid.net 网站来找到解决方法。另外，微软中文社区提供在线支持和定期专家聊天，都可以为我们解决问题提供宝贵的资源。

事件查看器日志分类

在事件查看器中共记录三种类型的日志。

1. 应用程序日志

包含有应用程序或系统程序记录的事件，主要记录程序运行方面的事件，录入数据库程序可以在应用程序日志中记录文件错误，程序开发人员可以自行决定监视的事件。

2. 安全性日志

记录了诸如有效和无效的登录尝试事件，以及与资源使用相关的事件。例如，创建、打开或删除文件或其他对象，系统管理员可以指定在安全性日志中记录什么事件。默认设置下，安全性日志是关闭的，管理员可以使用组策略来启动安全性日志，或者在注册表中设置审核策略，以便当安全性日志满后使系统停止响应。

3. 系统日志

包含 Windows XP 的系统组件记录的事件，例如在启动过程中加载驱动程序或者其他系统组件失败将记录在系统日志中。默认情况下，Windows 会将系统事件记录到系统日志之中。如果计算机被配置为域控制器，那么还将记录 DNS 服务器日志。当启动 Windows 时，“事件日志”服务会自动启动，所有用户都可以查看应用程序和系统日志，但只有管理员才能访问安全性日志。

事件查看器记录内容

在事件查看器中主要记录五种事件，事件查看器屏

幕左侧的图标描述了 Windows 操作系统对事件的分类。事件查看器显示如下类型的事件。

1. 错误：重大问题，例如数据丢失或功能丢失。如果服务在启动期间无法加载，便会记录一个错误。
2. 警告：不一定重要的事件也能指出潜在的问题。录入，如果磁盘空间低，便会记录一个警告。
3. 信息：描述应用程序、驱动程序或服务是否操作成功的事件。例如，如果网络驱动程序成功加载，便会记录一个信息事件。
4. 成功审核：接受审核且取得成功的安全访问尝试。例如，用户对系统的成功登录尝试将作为一个“成功审核”事件被记录下来。
5. 失败审核：接受审核且未成功的安全访问尝试。例如，如果用户试图访问网络驱动器未成功，该尝试将作为“失败审核”被记录下来。

用事件查看器解决故障案例

笔者利用 Windows 2008 Server R2 搭建 FTP 服务器后，使用 FlashFxp 连接 FTP 服务器时候，提示“数据 Socket 错误：连接被拒”的提示。根据以往的经验，出现这个错误是因为 FlashFXP 中没有去掉“被动模式”，我们只要需要去掉被动模式和关闭防火墙就可以了。

可我们将 FlashFXP 中的被动模式去掉以后，测试 FTP，问题同样存在。尝试很多办法也不能解决问题。

最后在事件查看器中，在“应用程序”的“事件属性”中发现一项事件为“事件 42，Serv-U FTP Server”，并且清楚表明，该事件级别为“错误”，事件 ID 为“42”，事件来源为“Serv-U FTP Server”及记录时间等，其中有一项提示“SERVER IS NOT LISTENING:Port number 21 is already in use!”（如图 1 所示）。

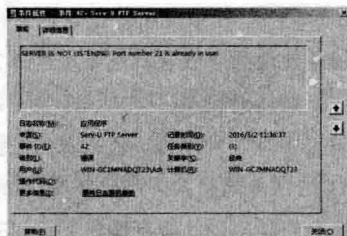


图 1 “错误”日志记录

然后我们就根据这些线索对 FTP 访问故障进行逐一排除。通过“开始→运行”，输入 CMD，进入 DOS 命令模式，在命令提示符下键入 netstat -ano 命令，来查看什么程序占用了 21 端口（如图 2 所示）。

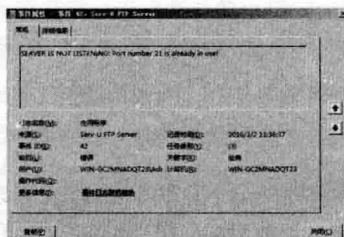


图 2 21 端口被占用

通过图 2 所示可以看到，图中端口号为 21，所对应的 PID 为 38908，接下来，需要找该 PID 对应的进程名称。

直接用命令查找，格式为 tasklist|findstr “38908” C:\>tasklist|findstr “38908”，结果发现映像名称为 tor.exe 占用了 21 端口。

首先结束该进程，具体方法为：在 DOS 命令提示符下输入：taskkill /f /t /im tor.exe。

再次进行 FTP 的连通性测试，完全正常。

经验总结

网管员通常苦于没有合适的第三方应用软件来解决各种系统故障问题，实际上 Windows 系统本身自带了很多优秀的小工具，而且有些小工具的功能非常强大，诸如垃圾清理、快速格式化、磁盘分区等。

本文利用 Windows 事件查看器所记录下的日志内容来发现 Serv-U 服务无法访问的根源，根据这一线索逐步排除最终解决问题。利用好了这些系统功能，不但系统的各种疑难杂症可以得到轻松解决，还有效地利用了系统资源。

两网串连故障

辽宁 冯志强

故障现象

节日过后第一天上上班，不同楼层的好几个部门打电话到值班室，说无法上综合网。为了不影响正常办公，单位迅速组织人员进行故障排除。

首先简单介绍一下单位网络拓扑结构。单位的网络分为综合网和办公网，且物理隔绝。综合网用于资料查询及娱乐学习；办公网用于日常办公。每个部门房间均有一个综合网接口和一个办公网接口。如图1所示，一楼主机房设置综合网主交换机（A1）和办公网主交换机（B1）及各自服务器，其他楼层分别设有若干两网交换机，连接各自楼层用户计算机。

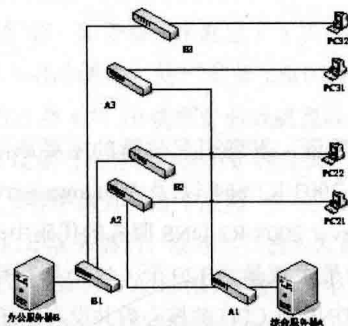


图1 办公网与综合网物理隔离

故障排查

用计算机 Ping 综合服务器和各楼层交换机，无法 Ping 通。怀疑主交换机 A1 死机了，于是进行重启。重启后，开始可以 Ping 通服务器，但不到一分钟又无法连通了，各楼层交换机始终不通。很明显，网络中产生了网络风暴。

采用排除法，在主交换机 A1 上，逐一插拔通往各楼层的网线。当拔掉通往二楼的网线时，网络恢复了正常。奇怪的是，二楼交换机还能 Ping 通。看来不是二楼自身产生环路，而是二楼与其他楼层之间产生了环路。

可能又有人私拉网线了。

为进一步寻找故障根源，保持通往二楼的网线断开，并逐一断开通往其他楼层的网线。当断开通往三楼的网线时，二楼、三楼同时断网。肯定是二楼、三楼之间产生了串连，从而产生网络环路的。

那么，如何判定是哪两个端口串连了呢？两楼层均有七八台交换机，端口有上百个，数量不小。幸好所有交换机都是可网管的，但也得一点点找。登录到二楼各交换机，发现在线用户并不是那么多。于是将在线用户端口逐一进行关闭和开启，直到无法连接二楼交换机为止。

经过半个多小时的尝试和努力，终于找到了串连端口。从配线架上找到对应部门房间号，来到问题所在房间，确实有一个私装的集线器，但并没有找到从三楼来的网线，问题出在哪里呢？仔细观察，集线器将从墙壁下来的综合网和办公网两条网线集合在一起，两台计算机也接在了集线器上。原来，办公人员想让两台电脑都上综合网，私自办公电脑上加了一个硬盘。办公时，用办公硬盘，接办公网；不办公时，用私加的硬盘，接集线器上综合网。当天早上没注意，把墙上下来的两条网线都接在了集线器上。从集线器上将办公网断开，并连接通往二楼的网线，全网恢复正常。

但仔细分析，问题并没有完全解决。两网串连虽然违规，但一处串连并不能产生网络环路，所以网络中还有一个串连点。为了证明这个推断，把综合网上一台计算机的 IP 地址改成办公网的，Ping 办公网服务器，果然通了。看来网络中确实还有一个两网串连点。那么，这个点在哪里呢？这个点应该在三楼，如图2所示。因为如果在二楼，当断开通往二楼的网线后，环路依然存在，网络不会恢复正常；如果在其他楼层，当断开通往三楼的网线后，二楼的综合网交换机不应该断网，所以只能是在三楼。

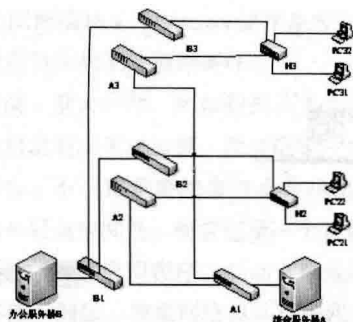


图 2 违规使用集线器 H2、H3，导致办公网与综合网物理连接

继续用综合网上的计算机 Ping 办公网服务器，逐一关闭和开启三楼办公网交换机端口，直到无法 Ping 通，找到所在问题部门房间，发现存在同样的问题，断开集

线器上的办公网网线后，网络彻底恢复。事后，对相关人员进行教育，并对各房间的网线进行了重新标记。

经验总结

通过本次故障排除，有以下几点启示。一是要加强网络制度管理，对办公人员进行网络知识普及。二是加强网络监测机制，及时发现两网串连事件的发生。三是建网初期要做好网络规划，预留出足够的拓展空间。四是对各种网络接口要做好标记，以便及时查找定位。五是增减网络设备时要在专业人员的指导下进行，并对网络拓扑资料进行及时更新。

安装群集遇麻烦

青 岛 李 佳 何 文 君

故障现象

最近，单位安装 Windows 2008 群集，安装环境为：两台 NF8560M2+ 存储+2 台光纤交换机。

结合项目，安装步骤大体为：a. 安装操作系统，b. 安装系统驱动，c. 安装系统补丁，d. 存储挂载和存储区域划分（仲裁+共享），e. 安装存储自带的客户端+Windows 自带的多路径（I/O）功能（服务器管理→功能→新增功能），f. 联机存储硬盘，添加盘符（仲裁和共享盘符通常为 X 和 Y，可以自定义），g. 群集配置（具体配置文档根据要安装的数据库可以从网上找下，重点是心跳网卡设置）。

但是，在本次安装的过程中出现了这样一个问题：建 AD 到最后的时候报错提示无法配置 DNS，RPC 服务器不可用，点“确定”和“完成”，DNS 服务器可以创建，但是 DNS 服务会自动关闭。查看事件日志显示，DNS 无法创建线程。

故障排查

经探讨验证，发现引起故障的主要原因为：在当前 Windows 2003 R2 x64 以及 Windows Server 2008 或 Windows Server 2008 R2 DNS 服务的代码中硬性规定了 DNS 线程的最大数量为 120 个（这个是写在代码中的）。但是，DNS 对 CPU 的核心数并没有作任何的限制，因此会创建超过 120 个线程。

具体来说，DNS 服务有 2 个功能的线程创建是根据 CPU 数量来决定的，一个是 DNS Dynamic update 功能以及 UDP I/O and dispatch 程序。在 64 核的机器上，它们会创建 64 个 Dynamic update 的线程和 64 个 UDP 处理线程。因此，在 64 核 CPU 的平台上，线程数量就会大大地超过限制的数量。 $64 \times 2 + (64/2 \text{ or } \text{NumberOfZones}) + 6 = \text{Max } 166 > 120$ ，因此就会报 ERROR_SERVICE_NO_THREAD 的错误。在 32 核的平台上，DNS 服务就工作正常，因为它最多创建 86 左右的线程。 $32 \times 2 + 16 + 6 = 86 \text{ threads}$ 。

本项目服务器配置 4 路 8 核 CPU，默认开启了超线程技术，实际 32 核可以模拟到 64 核（任务管理器→性

能一栏可以查看)。

故障解决

针对故障,我们最终是这样解决的:已经确认这个是 Windows DNS 服务的一个 Bug,我们惟一的选择是使用少于 48 核 CPU 的平台来提供 DNS 服务。 $48 \times 2 + 18 + 6 = 120$ (我们可以通过减少 AD 集成的 DNS 区域到 18 个来符合线程的限制)。当然,如果我们仅用 32 核 CPU,那就更没有问题了。

具体方法有两个:

1. 点击“开始→运行”,键入 msconfig,调出“系统配置”窗口,在“启动”选项里找到“高级选项卡”,更改 CPU 个数,改为 32。

2. 开机后进 BIOS → Advanced → Process&Clock → intel HT technology,把这个地方默认的 Enable 改成 Disabled。

修改完成后,在“任务管理器→性能”一栏,可以看到 CPU 数量已经调整为 32 个。

硬盘扩容出故障

福建泉州 王刚 曾玮琳 郑洪飞 孙延润

笔者单位曾对一台华为 FusionServer RH2285 服务器进行硬盘扩容。服务器原来配置了 5 块容量为 146GB 的 15000 转 SATA 硬盘,使用的是 LSI1064E REID 卡,并使用 RAID5 技术将 10 块硬盘做成磁盘阵列。后采购了 5 块 4TB 硬盘对原有硬盘进行扩容升级。

在升级过程中遇到了 2 个故障:一是硬盘在插入服务器插槽,启动服务器后,服务器扫描未发现任何硬盘。二是在故障一排除后,在 RAID 配置界面显示硬盘容量不正确,每块硬盘少了 2TB 的硬盘空间。

故障现象

故障一:将硬盘插入服务器硬盘插槽,启动服务器,服务器对硬盘进行初始化扫描操作,但当扫描结束后,所有的硬盘信号灯均显示红色(非正常),同时系统提示检测不到物理硬盘。

重启服务器后,进入 RAID 配置界面后,仍然未发现任何一块硬盘,也就是说 5 块新购硬盘都没有被系统识别到。

故障二:在故障一被排除后,进入 RAID 配置界面,所有的硬盘却只能识别到 2TB 硬盘空间,剩余 2TB 的硬盘空间却无法识别到,而在服务器开机自检的时候,

却可以识别到完整的 4TB 容量。

故障处理

1. 故障一的处理过程

首先对连接服务器和 RAID 卡的数据线进行了检查,然后将服务器 PCI 插槽中的 RAID 卡的线缆拔了下来连接到服务器主板的 SATA 接口,另一端直接连接新增的 4TB 硬盘。重启服务器,发现服务器可以正常识别硬盘,证明数据线正常。

接下来是检查 RAID 卡,担心在置换的时候因静电原因造成 RAID 卡损坏。采用硬件置换的方法对该服务器的 RAID 卡进行了置换,来检测 RAID 卡是否发生损坏。启动服务器后,服务器系统在检测扫描硬盘时,仍未发现硬盘,换回原来的 RAID 卡,连接原有 146GB 的服务器硬盘,可以正常识别所有硬盘。这样基本可以确定,RAID 卡没有物理故障。

第三,对新购硬盘进行了检查。对新购的物理硬盘,从主板上直接连接硬盘,逐一进行测试,发现其中一块物理硬盘无法识别,其余硬盘识别均正常。将可以正常识别的物理硬盘插入服务器插槽,然后恢复原有连接,启动服务器,发现所有的硬盘均可以正常识别。看来是

因为其中一块硬盘损坏，造成所有的硬盘都无法正常识别。

2. 故障二的处理过程

服务器只能识别 2TB 的硬盘空间，而不能识别 4TB 硬盘空间，我们采取了以下一些措施。

将原来的 146GB 硬盘更换回去后，所有的硬盘均可以正常识别，硬盘空间也均正常。经分析，认为可能是服务器对硬盘大小支持或 RAID 卡支持硬盘大小的问题，后进入华为官网，发现该服务器支持 SATA 硬盘，支持最大硬盘容量为 24TB，支持 RAID 0, 1, 10, 5, 6, 50 的数据保护技术，而新购硬盘总共大小为 $4 \times 4 = 16\text{TB}$ ，不存在超过服务器支持容量的现象。

接下来了解了一下该型号 RAID 卡的具体信息，发现 LSI1064E 型号的 RAID 卡只能识别 2TB 的硬盘，无法识别超过 2TB 的硬盘，看来只能更换 RAID 卡了。

后购买了一块 LSI2308 的 RAID 卡，所有的硬盘都可以正常识别，硬盘空间可以正常识别为 4TB，一切恢复正常。

经验总结

在安装新的物理硬盘时，如果有一块物理硬盘损坏，则有可能造成 RAID 卡无法正常识别所有的物理硬盘，这区别于服务器在正常使用中物理硬盘损坏的现象。服务器在正常使用过程中物理硬盘损坏时，其他正常工作

的硬盘是可以正常识别和使用的。

对于服务器无法正常识别硬盘容量，一般都是受主板、RAID 卡和 OS 软件所分别支持的寻址模式三个方面决定的。一般可以先查询服务器和 RAID 卡的支持信息来查看是哪个原因造成的。

对于 RAID 卡而言，对于硬盘空间的寻址方式决定了其可以识别和支持的磁盘容量。而 RAID 卡的寻址长度是基于 SBC 协议的 READ 字段来定义和决定的。对 LSI1064E RAID 卡而言，支持的协议为 READ (12)，寻址长度为 12 位（如图 1 所示）。其最大的寻址空间为 4byte，即 $2^{32} \times 512\text{B} = 2\text{TB}$ ，支持最大的单个硬盘空间为 2TB。故只能识别到 2TB 的容量，多余的容量不能被识别。正确识别的容量可以正常使用，建议使用单盘容量不超过 2TB 的硬盘。

Table 80 — READ (12) command

Byte	7	6	5	4	3	2	1	0
0	OPERATION CODE (A0h)							
1	READ/VERIFY		SPD	FLA	NRAC	FLA_INV	Obsolete	
2	(MSB)							(LSB)
3	LOGICAL BLOCK ADDRESS							
4								
5	(MSB)							(LSB)
6	TRANSFER LENGTH							
7								
8	(MSB)							(LSB)
9	GROUP NUMBER							
10								
11	CONTROL							

图 1 READ (12) 协议报文

而新购的 LSI2308 RAID 卡，支持的协议是 READ (16)，支持的寻址大小为 8 byte，故支持的单元盘容量大小为 $2^{64} \times 512\text{B} = 32\text{TB}$ 。

巧破数据包重传故障

福建泉州 王刚 曾玮琳 荣世辉

故障现象

笔者单位有很多下级单位，且各点位比较分散。一天，一个下级单位报告，在单位办公网站下载一个大约 3.4GB 的一个软件失败，然而在门户网站可以在线观看视频，但在观看电影时有明显卡顿和马赛克现象出现。

针对问题，笔者确定到下级单位的网络链路基本正常，首先怀疑可能是办公网站上的软件下载链接存在错

误。找到该软件的网站链接地址，无论是使用鼠标右键“目标另存为”还是使用迅雷等软件下载该软件均正常，说明该软件的下载链接没有问题，很可能是下级单位计算机操作系统存在问题。让下级单位更换几台计算机重新下载该软件测试，当使用鼠标右键“目标另存为”的方式下载时，过不了几秒，链接还是会中断，下载均失败。

为了解决问题，笔者使用“远程桌面”登录该计算

机,结果发现“远程桌面”无法正常建立,Ping了一下该计算机3389端口,丢包率为0,网络正常。笔者又使用65500字节大小的数据包Ping该计算机,丢包率高达33%,网络基本不可用。

故障排查

1. 根据故障现象和测试结果,笔者认为网络中可能存在广播风暴或ARP病毒等,造成网络阻塞,数据包超时丢失。遂对下级单位的所有上网计算机进行了病毒查杀,结果并未查杀到病毒。

2. 对所有的网络连接点进行了检查,发现各连接点并没有出现松脱、连接不紧密、线路短路等现象。

3. 因对下连接的网络特别简单,就是“计算机终端→交换机→光纤收发器→光纤收发器→交换机→计算机终端”的模式,对各网络设备进行了硬件测试,各网络硬件工作均正常,没有物理故障。

4. 对下级单位的网络流量数据包进行捕获,并对异常数据包进行分析,发现网络中并未出现病毒数据包和非合理广播数据包,惟一异常的数据包就是部分TCP发送异常,很多TCP数据包都产生了超时。对这些超时的数据包进行分析,发现错误提示为“在数据报组装期间生存时间为0”,也就是发生超时,TCP数据包重组失败。

故障原因

数据包发生超时重传的原因有很多,但是本故障中数据包发生重传的原因是TCP数据报文过大造成的。在IP数据包传输过程中,数据包首先要判断由哪个接口进行转发,并查询该接口的相关参数,以获得其MTU(Maximum Transmission Unit,最大传输单元),网络层把MTU值与要发送的IP数据包进行长度比较,如果IP数据包的长度比MTU值大(一般默认最大长度值为1500字节,MTU值不宜过大,也不宜过小,如果MTU配置过大,则可能会超过了接收端所能够承受的最大值,或者是超过了发送路径上途经的某台设备所能够承受的最大值,也会造成报文分片甚至丢弃,加重网络传输的负担,影响数据正常传输。MTU值过小的弊端在本文的最后有提及),就会对IP数据包进行分片处理,分片后的数据包长度小于或等于MTU值,当分片数据报文都到达目的端后,会对所有的分片数据报文进行重组,

当有一个分片或多个分片丢失后,就会造成数据报重组超时,所以就会发送超时的错误提示,导致TCP数据包传输异常。

导致数据重传一般有以下原因:一是计算机病毒和广播风暴。当网络带宽发生阻塞时,很多TCP数据包会被延时接收,当延时超过最大重传时间时,就会要求重传。二是网络设备设置不当和物理故障。当网络中存在多种网络设备时,有人会对各类网络设备设置不同的MTU,当各类网络设备的MTU不同时,可能就会导致数据包重传。比如,对路由器的MTU设置为1200字节,而交换机的MTU设置为800字节时,就有可能造成数据重传。三是网络线路原因。当各网络连接节点连接不紧密或网络链路出现其他异常故障时,也会造成数据包重传,而笔者单位发生这个故障就是光缆老化导致。

笔者单位到这个下级单位架设有超过38公里的光缆,光缆两端使用光纤收发器进行连接,来连通网络。光缆大部分采用的是埋地方式敷设,大约有9公里的光缆采用架空方式,虽然为铠装光缆,但使用时间已经超过17年,期间光缆断裂多次,光缆存在纤芯色散严重、油脂套管收缩严重、涂覆层油凝固、防水密封胶脱落、热缩套管破裂、光缆接续盒进水、外凯钢丝层和内径加强钢丝锈蚀等问题。特别是纤芯柔韧性降低明显,极易折断,使用OTDR(光时域反射仪)对光缆进行测试时,发现有多点和多段损耗较大,光缆老化非常严重,其中架空部分光缆老化尤其严重,即使单位使用了60公里的光纤收发器,光纤收发器经常不能很好地正常识别,导致数据收发异常。

数据包重传解决方法

因办公需要,要求对下网络中断时间不得超过1小时,为确保网络能符合办公要求,而此光缆又不可能立即重新敷设,笔者采取了三种解决方法。

1. 对损耗特别严重的光缆进行了更换。在对光缆进行测试后,发现其中有1段大约长2公里和1段大约长1.5公里的光缆损耗特别严重。在这两处敷设了新的光缆,对这两段的原有光缆进行了更换,熔接用时约25分钟。

2. 在提供的服务器上,对“最大重新传输超时”(RTO,Retransmission Timeout)、“最大传输单元”(MTU)和“最大重传次数”3个参数进行了修改(服务器采用Windows 2003 Server操作系统),这里将RTO设置为5000ms,将MTU设置为800字节,将“最大重传次数”

设置为 5 次。

(1) 修改 RTO 这个参数可以采用两种方法。

方法一：命令修改法。在操作系统中运行“cmd”命令，然后依次运行以下命令，netsh-interface-ipv4-show interface，可以查看到服务器外接的网络接口所对应的 Idx 值（如图 1 所示）。

```
netsh interface ipv4>show interface
```

Idx	Net	MTU	状态	名称
1	50	4294967295	connected	Loopback Pseudo-Interface 1
12	10	1500	connected	本地连接
14	20	1500	connected	VMware Network Adapter VMnet1
16	20	1500	connected	VMware Network Adapter VMnet8
19	20	1500	connected	VirtualBox Host-Only Network

图 1 网络接口所对应的 Idx 值

其对外服务的网卡接口名称为“本地连接”，其对应的 Idx 值为 12。使用“set interface "12" retransmittime=5000”命令就可以修改 RTO 这个参数为 5000ms，修改的命令和结果如下：

```
netsh interface ipv4>set interface "12" retransmittime=5000
```

确定。

方法二：修改注册表法。运行“regedit”命令打开注册表，分别打开 KEY_LOCAL_MACHINE\System\CurrentControlSet\Services\Tcpip\Parameters\Interfaces\适配器 ID（适配器 ID 可以根据对外网络的网址来确定（如图 2 所示），服务器中共有硬件或软件等各类“网卡”7 个，图中对外服务的为第三个，其网关为 192.168.1.1，自己的 IP 地址为 192.168.1.100），添加“TCPInitialRtt”名称的属性项，数据类型为 REG_DWORD，修改其数值为“5000”（即为 5000ms，5 秒）。



图 2 注册表编辑器界面

此参数控制 TCP 使用对每个新连接的初始重新传输超时。它适用于连接请求（SYN，synchronous）和每个连接发送的第一个数据段。

(2) 修改 MTU 这个参数可以采用命令修改法。在操作系统中运行“cmd”命令，然后依次运行以下命令，netsh-interface-ipv4，使用“set interface "12" mtu=800”命令就可以修改“最大传输单元”这个参数，修改的命

令和结果如下：

```
netsh interface ipv4>set interface "12" mtu=800
```

确定。

(3) 修改“最大重传次数”这个参数可以采用 2 种方法。

方法一：命令修改法。在操作系统中运行“cmd”命令，然后依次运行以下命令，netsh-interface-ipv4，使用“set interface "12" dadtransmits=5”命令就可以修改“最大传输单元”这个参数为 5 次，修改的命令和结果如下：

```
netsh interface ipv4> set interface "12" dadtransmits=5
```

确定。

方法二：修改注册表法。运行“regedit”打开注册表，分别打开 HKEY_LOCAL_MACHINE\System\CurrentControlSet\Services\Tcpip\Parameters，添加“TcpMaxDataRetransmissions”名称的属性项，数据类型为 REG_DWORD，修改其数值为“5”（即为 5 次）。

3. 在连接下级单位的交换机端口上，对该接口的 MTU 这个参数进行了修改（笔者单位使用的交换机为华为交换机，下级单位的交换机设置相同），修改相应接口 MTU 参数为 800 字节。

```
<HUAWEI> system-view
[HUAWEI] interface GigabitEthernet 0/0/5
[HUAWEI-GigabitEthernet0/0/1] undo portswitch
[HUAWEI-GigabitEthernet0/0/1] 800
[HUAWEI-Gigabit Ethernet0/0/1] restart
```

配置注意事项：需要在交换机端口执行命令 undo portswitch，配置以太网接口从二层模式切换到三层模式。同时在配置完成后，需要重启接口以保证配置的 MTU 生效。可以先执行命令 shutdown，关闭接口，再执行命令 undo shutdown，开启接口。也可以直接在接口视图下执行命令 restart，重启接口。

通过这些方法，可以很好地解决数据重传的问题，不会造成网络数据传输的中断。

但有利就有弊，这些方法的采用也存在一定的不足，主要不足体现在以下两个方面：一是采用了方法 2 和方法 3 后，会导致网络速度减慢。二是在设置了 QoS 的交换机上，由于 QoS 队列长度有限，如果 MTU 配置过小而报文尺寸较大，可能会造成分片过多，报文会被 QoS 队列丢弃，影响数据正常传输。

❖ 组播路由故障排除心得

福建泉州 李贵华

传统的 IP 传输只允许一台主机向单个主机或者所有主机发送报文，组播技术则提供第三种选择，即允许一台主机向某些主机发送报文。这些主机被称为组成员。发送到组成员的报文目的地址是某个 D 类地址 (224.0.0.0-239.255.255.255)。组播报文的传输类似于 UDP，只是一种尽力保证的服务，不提供类似于 TCP 的可靠传输和差错控制。平常我们接触到组播应用最多的是视频会议和视频点播等服务。笔者单位使用的 IP 会议终端就需要启用组播路由协议。本文介绍组播路由一般故障时的排除方法。

故障现象

一般来说，组播路由出现故障时，视频会议无法正常开会，或者就是声音图像卡顿现象比较明显，甚至出现长时间丢帧现象。排除故障的思路一般分为三步：一是检查网络是否正常，网络设备是否启用了组播路由协议。二是检查自治系统间组播路由是否正常。三是是否建立 MSDP 对等体。下面就对三个步骤进行详细分析。

步骤一：查看局域网交换机能否接收到组播包

通常情况下网络连接不正常，交换机未启用组播协议，组播应用程序没有加入到组播组这些因素都有可能引起收不到组播包这类故障。这种情况下，首先应检查局域网主机能否 Ping 通网关地址，如果不通，检查网络参数相关配置和物理连接，确保网络通信正常。其次，检查局域网交换机是否启用组播协议，组播协议分三层和二层，三层组播功能通常使用如下命令启用：

```
switch (config) #ip multicast-routing distributed
```

二层组播功能，有的厂商交换机默认启用，比如思科设备；有的需要手动配置，比如华三设备。可采用如

下命令查看是否存在二层接口和组成员：

```
switch# show ip igmp interface
```

```
switch# show ip igmp membership
```

如未启动二层组播功能，则输入下列命令启用：

```
switch (config) #igmp snooping
```

如果上述两步检查都正常，可能是交换机不转发组播包，可通过在交换机互联端口加入组播组的命令来实现组播功能。

```
switch (config-if) #ip igmp join-group X.X.X.X (组播地址)
```

步骤二：检查路由自治系统间组播路由是否异常

自治系统间的组播路由出现异常，通常是自治系统内没有设置统一的集合点 (Rendezvous Point, RP)，或自治系统边界未定义组播模式 (稀疏/密集)，又或是自治系统边界未设置 bsr-border 造成。解决的思路首先在本地图器上使用“Router# show ip pim rp”命令查看是否存在 RP。如果不存在 RP，说明 RP 设置有问题，可根据本网系的需求采用静态或手工指定 RP，全区域的 RP 地址必须一致。

静态 RP 配置命令如下：

```
Router (config) #ip pim rp-address X.X.X.X (RP 的 IP 地址)
```

动态 RP 配置命令为：

```
Router (config) #ip pim rp-candidate loopback 0 priority *** (priority 值越小越优先)
```

如果 RP 设置正确，自治系统间的组播路由依旧异常，使用“show interface”命令检查边界路由器之间的互联接口是否定义组播模式，若没有，在接口配置模式下增加如下命令：

```
Router (config-if) #ip pim sparse-mode (稀疏模式)
```

接着使用“show interface”命令检查边界路由器之间的互联接口是否设置 bsr-border, 若没有, 在接口配置模式下增加如下命令:

```
Router (config-if) #ip pim bsr-border
```

步骤三: 检查 RP 之间能否建立 MSDP 对等体

在不同 PIM-SM 域的 RP 之间不能建立 MSDP 对等体的故障一般都是未配置 MSDP Peer, 或配置的对等体与自治系统内的 RP 不一致造成。解决的思路首先在本 PIM 域的 RP 路由器上使用以下命令查看其 MSDP 对等情况, 其具体命名如下:

```
Router# show ip msdp peer
```

```
Router# show ip msdp summary
```

网络通信正常的情况下, 如果不存在 MSDP 对等体, 可使用“show running-config”命令检查路由器的 MSDP 协议设置项目是否正确, 如有错误, 更改该配置项。如果 MSDP 对等体与本自治系统的 RP 不一致, 将会导致不同的组播域无法建立对等关系。使用“show running-config”命令检查路由器配置文件中关于 RP 和 MSDP 的配置项, 若不一致, 则进行更改。

经验总结

通常我们在处理组播问题时, 应着重检查组播流经过的每一个设备和接口(包括 VLAN 接口), 这些设备和接口都必须配置组播参数。在检查的同时, 可借助组播测试工具, 分析判断组播数据中断于哪个设备的哪个接口, 以便确定故障点。

接口降级识别加密狗

▼ 石家庄 薛剑锋

故障现象

单位有一台 PC, 安装了 USB Over Network 服务器端, 用于共享 USB 设备。该 PC 共有 6 个 USB 接口, 其中 5 个口连接加密狗, 剩下的一个口用于连接 KVM。因其性能不能满足需要, 所以找了一台新的 PC 机(也是 6 个 USB 接口)将其替换。新 PC 上安装好 Windows 2008 系统和 USB Over Network 服务器端后, 从旧 PC 上逐一拔下 USB 加密狗, 插入到新 PC 的 USB 接口上并安装驱动, 结果第五个加密狗插入后无法识别。

故障原因

经过一番检查和测试, 发现原来新 PC 最后两个 USB 接口是 USB 3.0 的, 接 KVM 和 U 盘没问题, 但不兼容加密狗。

解决方案

由于该 PC 已无可用 USB 接口, 若要连接加密狗, 有两个办法, 一是接一个 USB Hub 到 2.0 接口上, 通常可扩展出四个 USB 接口。二是想办法将 USB 接口从 3.0 转换为 2.0, 也就是让操作系统把 3.0 接口识别成 2.0。

解决过程

经测试, 接 USB Hub 的办法可行, 只是有点儿影响美观。

如何将 USB 接口识别成 2.0 呢? 本人在网上找了一下, 有修改 BIOS 的, 也有修改 xHCI PCI Configuration Space 的。修改 BIOS, 一般是开机进如 BIOS 后, 在 Config-USB 菜单下, 将 USB 3.0 Mode 修改为 Disabled。只可惜在这台 PC 的 BIOS 里没找到相关的设置。于是我们采用另一种办法——修改 xHCI PCI Configuration Space。关于具体参数值的含义可参考 Intel 7 Series/C216

Chipset Family Platform Controller Hub 数据手册（注：下文简称 Intel 手册）。

此外，修改配置还需要用到一款软件——PCI Utilities。软件下载并解压到 C 盘后，以管理员身份打开命令行窗口，将当前目录切换到 PCI Utilities 文件夹。

下面会用到两个程序文件 lspci 和 setpci。lspci 用于显示 PCI 总线和设备的信息，setpci 用于修改 PCI 配置。

第一步，先用 lspci 查找 USB 3.0 接口信息。

```
C:\pciutils-3.4.0-win32>lspci -nn |find "xHCI">lspci.txt
```

```
00:14.0 USB controller [0c03]: Intel Corporation
7 Series/C210 Series Chipset Family USB xHCI Host
Controller [8086:1e31] (rev 04)
```

00:14.0 表示总线和插槽，8086:1e31 为厂商标识和设备标识，不同的设备可能标识也不同。

为更多地了解 setpci 命令的修改结果，也为了以后可以恢复设置，修改前先用 lspci 命令将 USB 3.0 控制器当前情况保存下来（如图 1 所示）。注意 d0 行的值，下面的修改影响的就是这一行。

```
C:\pciutils-3.4.0-win32>lspci -s 00:14.0 -xxx >lspci.txt
00:14.0 USB controller: Intel Corporation 7 Series/C210 Series Chipset Family USB
xHCI Host Controller (rev 04)
00: 86 80 31 1e 06 04 90 02 04 30 03 0c 00 00 00 00
10: 04 00 f0 f7 00 00 00 00 00 00 00 00 00 00 00 00
20: 00 00 00 00 00 00 00 00 00 00 00 00 25 10 30 80
30: 00 00 00 00 70 00 00 00 00 00 00 00 00 00 01 00
40: fd 07 0e 80 39 c2 03 80 00 00 00 00 00 00 00 00
50: 17 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
60: 30 20 00 00 00 00 00 00 00 00 00 00 00 00 00 00
70: 01 80 c2 c1 08 00 00 00 00 00 00 00 00 00 00 00
80: 05 00 b7 00 0c f0 ef fe 00 00 00 00 a8 49 00 00
90: 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
a0: 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
b0: 8f 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
c0: 03 0c 00 00 00 00 00 00 00 00 00 00 00 00 00 00
d0: 0f 00 00 00 0f 00 00 00 0f 00 00 00 0f 00 00 00
e0: 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
f0: 00 00 00 00 00 00 00 00 87 0f 05 08 00 00 00 00
```

图 1 保存 USB 3.0 控制器当前情况

第二步，关闭 USB 3.0 接口的 SuperSpeed 能力。

```
C:\pciutils-3.4.0-win32>setpci -H1 -d 8086:1e31 d8.l=0
（注：Intel 手册 17.1.35 部分这样描述：“When set to 0,
the port's SuperSpeed capability is not visible to the xHC.”）
```

查看 Configuration Space 的修改情况，如图 2 所示。

```
C:\pciutils-3.4.0-win32>lspci -s 00:14.0 -xxx >lspci.txt
00:14.0 USB controller: Intel Corporation 7 Series/C210 Series Chipset Family USB
xHCI Host Controller (rev 04)
00: 86 80 31 1e 06 04 90 02 04 30 03 0c 00 00 00 00
10: 04 00 f0 f7 00 00 00 00 00 00 00 00 00 00 00 00
20: 00 00 00 00 00 00 00 00 00 00 00 00 25 10 30 80
30: 00 00 00 00 70 00 00 00 00 00 00 00 00 00 01 00
40: fd 07 0e 80 39 c2 03 80 00 00 00 00 00 00 00 00
50: 17 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
60: 30 20 00 00 00 00 00 00 00 00 00 00 00 00 00 00
70: 01 80 c2 c1 08 00 00 00 00 00 00 00 00 00 00 00
80: 05 00 b7 00 0c f0 ef fe 00 00 00 00 a8 49 00 00
90: 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
a0: 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
b0: 8f 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
c0: 03 0c 00 00 00 00 00 00 00 00 00 00 00 00 00 00
d0: 0f 00 00 00 0f 00 00 00 0f 00 00 00 0f 00 00 00
e0: 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
f0: 00 00 00 00 00 00 00 00 87 0f 05 08 00 00 00 00
```

图 2 查看 Configuration Space 的修改情况

第三步，实现将连接到 USB 3.0 接口上的设备交由 EHCI 主控器处理。

```
C:\pciutils-3.4.0-win32>setpci -H1 -d 8086:1e31 d0.l=0
```

（注：Intel 手册 17.1.33 部分这样描述：“When set to 0, this bit routes all the corresponding USB 2.0 port pins to the EHCI controller (D29:F0) and RMH #1. The USB 2.0 port is masked from the xHC and the USB 2.0 port's OC pin is routed to the EHCI controller (D29:F0).”）

再次查看 Configuration Space 的修改情况，如图 3 所示。修改到此结束。

```
C:\pciutils-3.4.0-win32>lspci -s 00:14.0 -xxx >lspci.txt
00:14.0 USB controller: Intel Corporation 7 Series/C210 Series Chipset Family USB
xHCI Host Controller (rev 04)
00: 86 80 31 1e 06 04 90 02 04 30 03 0c 00 00 00 00
10: 04 00 f0 f7 00 00 00 00 00 00 00 00 00 00 00 00
20: 00 00 00 00 00 00 00 00 00 00 00 00 25 10 30 80
30: 00 00 00 00 70 00 00 00 00 00 00 00 00 00 01 00
40: fd 07 0e 80 39 c2 03 80 00 00 00 00 00 00 00 00
50: 17 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
60: 30 20 00 00 00 00 00 00 00 00 00 00 00 00 00 00
70: 01 80 c2 c1 08 00 00 00 00 00 00 00 00 00 00 00
80: 05 00 b7 00 0c f0 ef fe 00 00 00 00 a8 49 00 00
90: 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
a0: 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
b0: 8f 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
c0: 03 0c 00 00 00 00 00 00 00 00 00 00 00 00 00 00
d0: 0f 00 00 00 0f 00 00 00 0f 00 00 00 0f 00 00 00
e0: 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
f0: 00 00 00 00 00 00 00 00 87 0f 05 08 00 00 00 00
```

图 3 再次修改 Configuration Space 的情况

将加密狗接到 USB 3.0 接口，系统顺利地识别出来。

恢复办法

```
C:\pciutils-3.4.0-win32>setpci -H1 -d 8086:8c31
d8.l=0f
```

```
C:\pciutils-3.4.0-win32>setpci -H1 -d 8086:8c31
d0.l=000f
```

不过，新的问题又出现了。系统重启后，上面的设置会失效。解决办法是，写一个批处理程序 usb3to2.bat，内容如下：

```
C:\pciutils-3.4.0-win32>setpci -H1 -d 8086:1e31 d8.l=0
```

```
C:\pciutils-3.4.0-win32>setpci -H1 -d 8086:1e31 d0.l=0
```

然后添加计划任务，让系统启动时执行 usb3to2.bat 即可。

关于 USB Over Network

这是一个功能强大可靠、使用方便的 USB 设备共享解决方案，可以允许分享和获取本地或者网上的 USB 设备。可以通过网络远程访问指定的 USB 接口的软件。分为 USB Over Network Client 和 USB Over Network Server。Server 相当于服务器端安装在提供 USB 内容的

电脑上, Client 相当于客户端安装在其他电脑上用来访问 Server 端的 USB 内容。在 Client 上输入 Server 端电脑的 IP 地址就可以访问。

Intel 7 Series/C216 Chipset Family Platform Controller Hub 数据手册下载地址:

<http://www.intel.com/content/dam/www/public/us/en/documents/datasheets/7-series-chipset-pch-datasheet.pdf>

PCI Utilities 下载地址:

<https://eternallybored.org/misc/pciutils/>

路由汇聚引发网络故障

青岛 廖方旭 蒋鑫晖 曹茂虹

笔者所在单位计划将甲乙两套 IP 网络使用 BGP MPLS VPN 技术进行调整, 使不同网络的纵向业务能够使用一条物理线路进行逻辑隔离, 达到资源节约和便于管理的目的。调整前的甲、乙部分网络是相互独立的(如图 1 所示)。

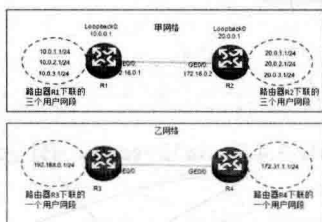


图 1 网络调整前的甲网络和乙网络

此次调整是基于甲网络进行的, 调整后乙网络的设备和线路取消, 调整时将之前乙网络中的 192.168.0.1/24 和 172.31.1.1/24 划入调整后网络的 VPN 实例 1 中(如图 2 所示), 两段网络能够互通, 并与 VPN 实例 1 外的网络隔离。



图 2 调整中的网络（甲乙网络使用一套物理线路）

故障现象

在 PE1 路由器上能够看到位于 VPN 实例 1 中的

172.31.1.0/24 的 BGP 路由, 但是 Ping 不通 172.31.1.1 (172.31.1.0/24 的网关)(如图 3 所示)。

```

<PE1>#show ip routing-table vpn-instance 1
Routing Tables: 1
Destinations: 5
Routes: 5

Destination/Mask    Proto Pre  Cost      NextHop    Interface
-----
127.0.0.0/8         Direct 0     0          127.0.0.1   InLoop0
127.0.0.1/32        Direct 0     0          127.0.0.1   InLoop0
192.168.0.0/24      BGP     255    0          192.168.0.1  eth0/1
192.168.0.1/32      Direct 0     0          192.168.0.1  InLoop0

<PE1>#ping -vpn-instance 1 172.31.1.1
PING 172.31.1.1: 36 data bytes, press CTRL_C to break
Request time out
Request time out
Request time out
Request time out
Request time out

--- 172.31.1.1 ping statistics ---
 5 packet(s) transmitted
 0 packet(s) received
100.00% packet loss
    
```

图 3 可看到 172.31.1.0/24 的 BGP 路由, 但 Ping 不通

故障排查

按照 BGP MPLS VPN 的排错过程进行故障排查。

1. 检查公网隧道是否存在

检查公网路由学习是否正确, 能发现对方的 loopback0 地址路由, 并且能够 Ping 通。

检查公网设备之间的 MPLS LDP 邻居关系是否正常, 发现 PE1 和 PE2 之间能够建立正常的 MPLS LDP 邻居(邻居状态为 operational)。

检查公网隧道是否存在, 发现 PE1 和 PE2 之间的公网隧道正常。

2. 检查本地 VPN 建立是否符合要求

检查 PE1 上的 192.168.0.1/24 网段已经通过 ip binding vpn-instance 1 命令绑定到 VPN 实例 1 中, PE2 上 172.31.1.0/24 的网段也已绑定到 VPN 实例 1 中, 并且网段的端口都为 UP 状态。

3. 检查 MP-BGP 私网路由传递是否正确

检查 PE 之间 MP-BGP 邻居是否建立成功，发现 PE1 和 PE2 之间能够建立正常的 MP-BGP 邻居（邻居状态为 Established）。

检查 PE 是否学习到远端用户的私网 BGP 路由，发现 PE1 能够发现 PE2 上 172.31.1.0/24 网段的 BGP 路由，但 PE2 不能发现 PE1 上 192.168.0.1/24 网段的 BGP 路由。

故障排除与分析

鉴于以上故障排查过程，只能再次查看 PE1 和 PE2 的配置，发现由于 PE1 的 loopback0 地址为 10.0.0.1/32，而路由器下有三个用户网段，分别为 10.0.1.0/24、10.0.2.0/24 和 10.0.3.0/24，为减少路由条目，使用了路由汇聚命令。将三条路由汇总为一条 10.0.0.0/22 的路由（如图 4 所示），loopback0 的地址也被汇总为该条路由，此时，PE-2 公网上只能收到一条 10.0.0.0/22 的汇总路由。

```
<pe1>dis cu conf ospf
#
ospf 1 router-id 10.0.0.1
area 0.0.0.0
abr-summary 10.0.0.0 255.255.252.0
network 10.0.0.1 0.0.0.0
area 0.0.0.1
network 172.16.0.0 0.0.0.3
#
return
```

图 4 路由汇聚配置

查阅 MPLS 的相关资料，根据 MPLS 的相关概念，一个 FEC（转发等价类）只会为同一个路由分配标签，沿途所有的设备都必须具有相同的路由（前缀和掩码必须完全相同）才可以建成一条 LSP。

在此次调整的网络中运行 MPLS VPN 的两台 PE 的 loopback 地址分别作为对端的 next-hop 地址存在，MPLS VPN 外层隧道的源与目的分别是两台 PE 的 loopback 接口并以此建立 FEC，但是 PE2 没有到 PE1 loopback0 10.0.0.1/32 的精确路由，所以没能建立一条 LSP。

因此，使用 MPLS 转发的所有设备上，对于要使用标签转发的路由，都不能做路由聚合的操作。因此这个 32 位的主机地址需要精准指定，避免被错误聚合。

将 abr-summary 10.0.0.0 255.255.252.0 这条命令去除后，就能正常 Ping 通 PE2 上的 172.31.1.1 了。

修复网站服务器

辽宁锦州 冯志强

单位有一台网站服务器，主要用于信息发布、新闻浏览、音视频下载等，同时兼做邮件服务器，为单位人员提供文件流转服务。服务器购于 2008 年，运行一直很稳定，所以平时很少进行维护。但最近却经常出现异常，以致最后无法启动。

故障现象

近期，单位经常有人反映网站邮件服务界面无法登录，不能进入电子邮箱。这种情况一般重启服务器或重启“IIS Admin Service”和“WinWebMail Server”就能恢复正常。但渐渐发现，服务器重启时间比以前长了很

多，终于有一天，服务器重启后无法进入系统，当运行到 Windows 2003 欢迎界面时反复自动重启。在 BIOS 里无法发现硬盘，初步判断为硬盘故障。

故障排查

由于服务器上存有整个网站源代码、相关资料和邮件数据文件等重要数据，所以首先要进行数据备份。虽然以前备份过，但时隔一年多，内容改动较大，特别是邮件服务中，涉及到很多用户的即时数据。此服务器只有一个硬盘，因此没有 Raid 设置。

用 PE 盘进入服务器的 PE 系统，发现硬盘共两个分

区:C盘和D盘。C盘无法打开,而且无分区大小信息。D盘可以打开,但耗时很长。操作系统在C盘,网站和邮件服务器的数据都在D盘,看来可以先进行数据备份,再进行其他操作。

在复制文件时,系统提示要几天时间才能复制完成,明显不正常,而且过十几分钟就弹出无法复制。用DiskGenius硬盘分区及数据维护软件打开硬盘,选择D盘,对需要备份的数据进行备份。

虽然所需数据备份出来了,但在备份过程中,还是提示了几次因磁盘存在柱面信息丢失而跳过了一些部分。

有了备份数据,准备重新换一块新硬盘架设服务器,但网站维护人员说需要一段时间才能完成,让先看看能不能把硬盘修好。既然数据已经备份,可以对故障硬盘进行尝试性修复了。在DiskGenius软件中,发现原来C盘的内容也能进行浏览,只是从系统的资源管理器中无法打开。看来C盘也不是完全损坏,可能是分区表出现了故障。重建分区表并保存,在资源管理器中还是无法显示C盘信息。

故障排除

在系统中运行CMD,打开DOS界面,输入:CHKDSK C: /F,再输入回车,检查磁盘并修复磁盘上

的错误。检查过程中,出现了很多磁盘错误信息并进行了修复。检查完毕后,发现C盘竟然可以打开了,看来确实是分区表出现了问题。又对D盘进行检查,也出现了许多磁盘错误并进行了修复。

把硬盘接回服务器后开机,系统又自动对磁盘进行了检查和修复后正常启动。又重启了几次,均能正常开机,网站和邮件服务也能正常使用。看来服务器可以暂时使用,等新的服务器架好后进行更换。

经验总结

通过本次网站服务器修复经历,得到了很多启示。

1. 对于重要的网络设备和服务器等,要进行及时维护。当出现不正常现象时,应及时彻底查明原因,进行维护或更换,不能等到发生故障时再维修。

2. 对服务器中的重要数据要定期及时备份,防止因突发故障造成重要数据无法恢复,或因时间过长,造成已备份的数据失出时效性。

3. 服务器应采用硬盘阵列进行存储,比如做成Raid 1或Raid 5,防止因某块硬盘故障造成系统崩溃。

4. 对服务器存储设备进行修复时,首先应保护重要数据,进行数据备份,然后再对硬件进行维修,防止因维修不当造成重要数据丢失。

被遗忘的路由

青 岛 丁 炜 朱 俊 翰

最近单位发生一起奇怪的网络故障,问题原因很简单,但找到问题却颇费周折。

先介绍一下我单位市局城域网的基本情况。

七个区市局共十个办公地点,通过MSTP专线与

市局连接,其中两个区市局(区市1、区市10)的互联网出口也在市局。市局互联网出口有两条,一条是联通100M,一条是电信10M。市局新上上网行为管理设备(如图1所示)。

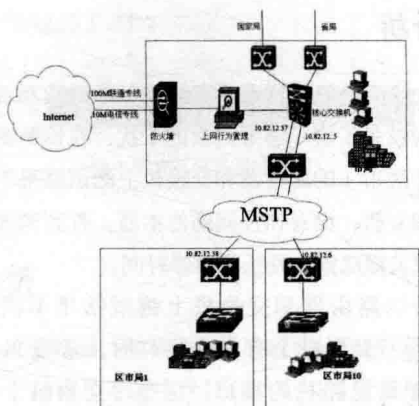


图 1 全市拓扑结构

防火墙接口配置说明：Eth10 电信互联网出口、Eth11 联通互联网出口、Eth12 内网口、Eth13 DMZ 区（如图 2 所示）。

eth10	接口/端口/100M	219.147.6.82/255.255.255.248
eth11	接口/端口/100M	221.215.210.154/255.255.255.248
eth12	接口/端口/1000M	172.18.226.251/255.255.255.0
eth13	接口/端口/100M	192.168.6.234/255.255.255.0

图 2 防火墙接口配置

故障现象及处理

某日，区市一位工作人员反映不能连接互联网，访问市局、省局等正常。

初步分析：

除区市 1，其他区市局用户访问互联网均正常，说明互联网线路没有问题。

将区市 1 与区市 10 路由器、交换机的配置做对比未发现异常。

由于以前网络运行一直平稳，这次故障是新上的上网行为管理设备后发生，于是跳过上网行为管理设备直接通过防火墙访问互联网，这时发现区市 1 访问互联网恢复正常。第二天将上网行为管理设备又重新接入，区市 1 访问互联网正常未受影响。

一段时间后，一天晚上，区市 1 访问互联网又完全断掉，第二天自行恢复。

几天后，区市 1 访问互联网又断掉，这次采取以下措施均不奏效。

1. 隔离上网行为管理设备。
2. 重新启动区市 1 网络设备。
3. 区市 1 交换机上的计算机连接网线全部拔掉，在市局远程 telnet，测试。

以上措施可排除内部病毒和网络攻击及上网行为管

理设备造成的故障。

这次故障排查测试时，发现在区市 1 的路由器和交换机上 Ping 市局互联网出口结果不同：路由器 Ping 市局防火墙上的联通外网互联地址 221.215.210.153 可达，交换机 Ping 市局防火墙上的联通外网互联地址 221.215.210.153 不可达。而且在区市 1 交换机上 traceroute 市局防火墙的外网地址，只能跟踪到内网口地址，这表明区市 1 的路由配置没有问题，问题出在市局的防火墙上，市局的防火墙收到了来自区市 1 网段 10.xx.83.0/24 的互联网连接请求，但不能转发到互联网出口。

可是为什么其他网段的流量转发正常呢？到防火墙管理界面仔细查看才发现，互联网出口的电信线路是不可达的，有一条在界面上非常隐蔽的策略路由（网络管理——路由 - 策略路由 a 中的一条路由）将区市 1 的流量分配到电信线路。联系运营商说因线路欠费被关闭，线路重新开启后，一切恢复正常。

恢复测试

故障恢复后又做测试如下：

1. 电信线路正常时，在城阳区的交换机上跟踪互联网地址：

```
Sw-ChenYang> traceroute 101.69.104.74
```

```
Type escape sequence to abort.
```

```
Tracing the route to 101.69.104.74
```

```
1 10.82.83.1 0 msec 0 msec 8 msec
2 10.82.12.37 0 msec 0 msec 0 msec
3 172.18.226.251 0 msec 8 msec 0 msec
4 219.147.6.81 17 msec 0 msec 8 msec
5 222.173.65.41 0 msec 9 msec 0 msec
6 ...
```

```
15 * * *
```

```
16 101.69.104.74 109 msec 109 msec 109 msec
```

2. 将市局防火墙上电信互联网接口的网线拔掉时：

```
Sw-ChenYang> traceroute 101.69.104.74
```

```
Type escape sequence to abort.
```

```
Tracing the route to 101.69.104.74
```

```
1 10.82.83.1 0 msec 9 msec 0 msec
2 10.82.12.37 8 msec 8 msec 0 msec
3 172.18.226.251 9 msec 0 msec 8 msec
4 221.215.210.153 0 msec 9 msec 8 msec
5 119.167.125.121 0 msec 8 msec 0 msec
```


6...

10 221.12.82.194 42 msec 25 msec 34 msec

11 * * *

12 * * *

13 101.69.104.74 25 msec 33 msec 34 msec

此时, 因为电信互联网出口为 Down 的状态, 防火墙会跳过策略路由, 将包转发到联通出口 221.215.210.153。

3. 关闭机房电线互联网线路的光纤收发器 (模拟远端线路故障)

Sw-ChenYang> traceroute 101.69.104.74

Type escape sequence to abort.

Tracing the route to 101.69.104.74

1 10.82.83.1 0 msec 0 msec 0 msec

2 10.82.12.37 17 msec 9 msec 0 msec

3 172.18.226.251 8 msec 0 msec 0 msec

4 * * *

5 * * *

6 * * *

...

30 * * *

此时, 电信互联网出口为 Up 的状态, 但对端地址 219.147.6.81 不可达, 就出现了类似前期欠费断网的情况。

故障分析

这次故障处理受到运营商线路时停时续和对新网络上网行为设备了解不够等因素的干扰, 在诊断测试时虽然发现在区市 1 的路由器和交换机上测试结果不同, 也没有仔细分析, 没有抓住问题的本质。直到彻底断网才重新审视关键线索, 延长了维修时间。

之所以路由器和交换机上测试结果不同, 是因为路由器、交换机上有多个接口时, 常规 Ping 的时候会选择最短路径的接口, 区市 1 交换机上全部是 10.xx.83.0/24, 它的包到达防火墙后被转发到了电信互联网出口, 电信线路此时断掉, 所以 Ping 联通互联网 100M 互联地址时不通。而区市 1 路由器最短路径的接口 (10.xx.74.7) 的包到达防火墙后被转发到联通互联网 100M 出口, 自然 Ping 与其直联的联通互联网 100M 互联地址时是通的。

经验总结

通过这次事件得到以下提示, 要快速高效的进行网络故障排除, 网络管理人员一定要有扎实的基本功, 深入学习底层协议和网络设备的通信原理, 判断时笃信不疑才能少受各种意外现象影响。网络配置要专人负责, 配置及修改要有详细记录文档, 临时测试的配置要即用即删。管理人员要整理完备详细的网络系统档案, 网络有变动时及时更新。

❖ 抓出交换机系统 Bug

福建泉州 王刚 程玉青 梁国君

故障现象

笔者接到一个朋友求助, 所在公司新建网络使用华为 S5700-28C-EI-24S 交换机 (该交换机于 2012 年 2 月生产) 作为对上连通交换机。在进行系统和业务试运行, 发现交换机的上联端口存在数据间歇性爆发现象。

从网管系统上看到该端口每隔 7 秒左右转发一次大

流量数据, 然后接着 7 秒左右数据收发正常, 这个现象一直循环重复出现, 在网管系统中的流量波形图如图 1 所示。此外, 在网络中发现大量的广播数据包。更为严重的是, 这种现象在持续了近 2 个小时后, 交换机会自动重启, 交换机重新启动后又出现上述现象。又过了 2 小时, 交换机又自动重启, 严重影响系统正常运行。登录该交换机, 使用 display cpu-usage 命令, 发现交换机

CPU 使用率超过了 72%。



图 1 网管系统流量波形图

故障分析

根据故障原因，笔者分析了造成该故障的可能原因。一是试运行的应用系统本身原因。应用系统本身存在设计问题时，数据存在间歇性地发送大量数据设计，从而导致交换机流量异常和重启。二是病毒导致。网络中存在木马病毒，会周期性地触发用于木马病毒传播的流量。三是网络中存在广播风暴。可能因为病毒或存在环路，网络中存在大量的广播包，造成网络阻塞。四是交换机 ISO 存在 Bug。当 ISO 存在 Bug 时，会对部分数据进行缓存，到了临界点时，再一次性进行短时间内的瞬时转发，当交换机无法处理大量的数据时，就会造成死机和重启。

故障排查

- 1. 对应用系统服务器进行了流量监控统计。在应用系统服务器出入接口进行了流量统计，发现服务器进出流量波形图基本处于平滑，每秒进出服务器的数据相差不大，不存在流量突变情况，排除了应用系统设计不足故障。
- 2. 对网络中所有的用户终端进行了木马病毒查杀。使用了最新的杀毒软件对所有的用户终端查杀了木马病毒，虽存在有病毒，但并未发现会造成异常流量和广播风暴的木马病毒。

- 3. 检查了网络链路。通过使用交换机环路检测命令和对所有的链路节点进行检查，没有发现存在物理网络环路。
- 4. 抓包验证。采用了全镜像、输入流量、输出流量三种抓包方式进行流量统计。对上联端口的进出流量进行了全镜像抓包。在抓了 3 分钟 30 秒后，发现流量传输波形比较平滑，没有出现转发的中断和流量突发（如图 2 所示）。



图 2 交换机全镜像流量波形图

对上联端口的接收流量进行了全镜像抓包，并进行分析，抓包后的接收流量波形图如图 3 所示。可以看到，接收的流量波形图是基本平滑的，其波峰不存在较大异变。

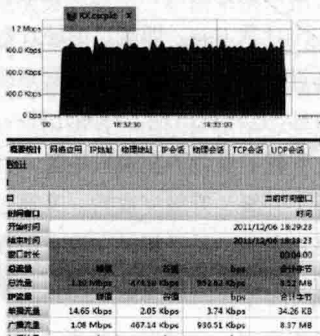


图 3 交换机端口接收镜像流量波形图

对上联端口的发送流量进行了全镜像抓包，并进行分析，抓包后的发送流量波形图如图 4 所示。可以看到，发送的流量波形图存在较大异变，但其异变周期为 10 秒左右，而非 7 秒。通过抓包发现，在发送的流量中出现一些流量的峰值，但其异变峰值平均只有 173Kbps，而在网管系统中出现的峰值平均值却高达 400kbps，看来发送的流量不是造成故障的主要原因，应该属于正常现象。

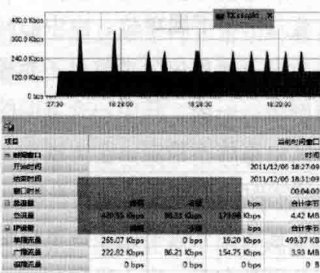


图 4 交换机端口发送镜像流量波形图

通过抓包，发现网络中存在大量的广播包，流量中的单播数据很少，跟日常的流量相比显得怪异，流量的转发大部分都为广播包。后经过询问得知，网管控制系统在设计的时候就采用的是全网广播的形式进行数据的交互，因此产生大量的广播包也属正常。

此外，通过抓包还发现，无论采用哪种抓包方式，都可以看到流量是平滑的，没有出现过流量的波动较大情况，也没有出现流量转发中断的情况，这与网管软件和交换机端口看到的流量统计情况完全不一样。出现这种情况，基本可以判断，这种现象应该是交换机系统存在 Bug。

故障排除

升级交换机系统。登录华为官网，发现华为 S5700 系统交换机存在系统 Bug，在 Bug 描述中，老版本系统在处理全网广播的数据的时候会出现 Bug，在网络流量统计时存在一个计数 Bug，即端口的统计数据包不是实时统计，而是过几秒统计一次，而网管系统读取的是交换机的端口信息，这样就出现了每隔几秒一次的波形图。

在网站上下载了最新的交换机系统文件，对该交换机的系统进行了升级，升级完成后，又通过抓包了解到数据的转发是正常的，是平滑的，没有出现网管系统中的波形图，网管系统中的流量波形图也正常，交换机端

口的流量统计也正常，故障排除。

经验总结

交换机镜像技术本身是一门很底层的技术，是在芯片级别实现的，也就是说使用该技术时，进出端口的数据流量会在进出系统处理之前就会对流量进行镜像。

因此，通过镜像我们可以看到流量在进出该端口的底层数据上是平滑的，而通过网管系统和交换机统计的流量不完全一致时，基本可以确定是交换机系统存在 Bug。

进水导致光纤链路异常

福建泉州 王刚 郑洪飞 余鑫海

故障现象

笔者单位有几十个下属单位，由中心网络机房分别向 4 个方向给所有下属单位分别敷设了光缆，并使用光纤收发器连通网络。一天，其中一个方向的所有下属单位均报告办公文电系统不稳定，会出现登录系统后不久掉线、登录系统需时较长或无法登录系统等现象。

这个方向共有 9 个下属单位，各单位距离中心网络机房大约只有几百米左右，中心机房到这个方向敷设有 1 条 72 芯光缆，在其中一个单位室外架设有 1 个网络机柜，内装有光缆配线架，从这个光缆配线架分别向其他 8 个单位各敷设有 1 条 8 芯光缆。

网络不稳定因素

1. 线路问题

光缆导致网络时断时续主要有 4 个因素，第一个因素是光缆制造工艺不良，极易在光缆接续点附近出现光纤劣化，随着时间变久，光缆接续点处会出现衰耗急剧增大的现象。第二个因素是光纤敷设时，光缆受机械力牵引等原因产生扭伤、弯折而产生断裂但尚未断开。第

三个因素是光缆埋设到地下时，受其他施工影响、车辆碾压、虫咬鼠啃、光缆接续点保护管安装存在问题等原因导致光缆断开但尚未断开和接头盒漏水等。第四个因素是各光缆连接处受外力，造成连接处脱连或连接不紧密。

2. 病毒问题

当网络中存在有 ARP 病毒时，会导致网络出现时断时续。

3. 广播风暴

广播风暴会导致网络时断时续，出现广播风暴的原因主要是临时架设网线造成环路导致广播风暴。

4. 硬件问题

所有的网络设备包括交换机、网卡等在长时间使用，都会出现故障。笔者经常有碰到交换机刚开始使用比较正常，当数据流量过多或长时间工作时，交换机会出现时断时续和假死现象，往往需要重启一下才可以恢复正常。

5. 软件问题

软件问题一般都是因为计算机安装了新的应用程序，导致办公系统的端口被占用，端口冲突导致网络应用系统无法正常使用。

6. 环境问题

环境问题也是造成网络设备不稳定的主要原因, 比较突出的因素有静电干扰、供电电压不稳、网络设备散热不良等。很多末端网络设备电源都不接地线, 再加上附近其他电器干扰, 网络设备极易被干扰, 网络设备会不稳定, 网络业务会出现时断时续, 严重时会造成掉线。

故障排查

在询问了下属单位的故障现象后, 笔者采取了“步步排除, 先易后难”的方法进行故障排除, 了解到下属单位办公计算机未安装新的应用程序、各网络机房均未安装新设备及未对各类线路进行改造后, 开始排除故障。

1. 排除广播风暴因素

笔者在中心机房使用计算机 Ping 下属单位的计算机, 发现掉包非常严重, 丢包率高达 90% 以上, 成功的数据包其时延也高达 2000ms 以上, 网络基本上无法正常使用。让所有下属单位计算机内部互 Ping, 不仅没有丢包, 而且延时均小于 1ms, 也就说明下属单位内部不存在广播风暴。

2. 排除交换设备故障

9 个下属单位均有 1 台交换机, 同时出现故障的可能性几乎为零, 但这 9 个下属单位连接在中心机房的同一台交换机上, 遂判定此交换机可能出现故障, 在将这台交换机重新启动后, 故障依旧, 后又更换了一台新交换机, 故障仍未排除。将更换下来的交换机进行了端口测试, 交换机运行正常, 说明故障不是由交换机引发的。

3. 查杀病毒

对下属单位的办公计算机的病毒库进行了升级, 利用杀毒软件和 ARP 专杀工具对所有的办公计算机进行了全盘杀毒操作, 并未查杀到 ARP 病毒和其他病毒, 故障仍未排除, 遂认定可能为线路故障。

4. 排查线路

第一步是在中心机房, 对到这个方向所有的网络连接点进行了检查, 同时要求各下属单位对自己机房内的尾纤、耦合器、配线架及 RJ45 水晶头等连接点进行检查,

发现各连接点连接均正常。第二步是在中心机房发现到各下属单位的光纤收发器运行指示灯均正常, 没有出现指示灯异常现象, 光缆不存在断裂现象。第三步是对其中一个无法登录系统的下属单位光缆进行了简单检查, 检查结果光缆没有断裂。第四步是使用光时域反射仪对各光路进行检测, 发现在距离各下属单位 50-100 米不等处有明显的菲涅尔反射峰, 查看光缆敷设资料后, 遂判断为下属单位的室外网络机柜中安装的光缆配线架出现了故障。

故障排除

当找到那个光缆配线架时, 发现室外网络机柜外部被撞击发生了变形和破损, 雨水渗透进网络机柜, 光缆配线架同各耦合器连接头均被雨水浸泡。立刻清洁接线箱内的所有光缆接头和耦合器连接头, 利用电吹风加热干燥了光缆接头和耦合器接头, 重新更换了室外网络机柜, 故障彻底消失。

经验总结

此故障是因网络机柜进水, 机柜内的光纤耦合器被雨水浸泡, 导致在对接头处发生了光反射, 来回的强反射信号经过较少的衰减后与正常信号叠加, 破坏了传输数据的正常结构。

在长距离链路情况下, 即使存在反射信号, 也不会对数据接收造成严重影响, 但如果链路过短或采取的终端光模块信号过强时, 就可能会导致数据错误率上升, 网络速度变慢, 严重时甚至不能实现光链路的联通。

一般来讲, 链路越短, 速度越高, 光模块功率越大, 网络受影响的程度也就越严重。在天气晴朗时, 因水分蒸发, 网络会相对稳定。当遇到天阴或下雨天气时, 网络会变得不稳定, 严重时, 网络甚至会出现中断现象。遇到这种现象时, 可以先从排除室外光缆连接故障开始, 再排除其他故障。

机房搬迁网不通

天津 郁成军 吴线美子 蒋铁军 曹国强 张慧伟

故障现象

我单位因为业务拓展需求，要搬迁其中一个下属站点机房。总部与该站点之间的网络拓扑结构如图 1 所示（为简洁起见，未画出两个机房的光端机）。搬迁后，该站点与总部之间的网络连接关系保持不变，只是原来由本单位维护的 2M 线路改为租用电信公司的 2M 线路。这就意味着，线路两端的路由器不需要修改参数配置。这项工作并不复杂，设备搬至目的机房，正确连接后加电，网络即可连通。

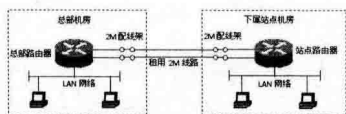


图 1 网络拓扑图

由于这项工作相对简单，且工作量不大，起初没有引起足够的重视。新机房整治完毕，2M 线路调通，搬迁工作开始。设备正确连接后加电，然而，网络却未能如愿连通。单位领导先后两次派人排查未果。

故障排查

笔者带领抢修小组，再次进行故障排查。首先通过 Ping 命令检查总部局域网及外网之间的连通性，局域网内部畅通；外网除该站点外均畅通。经该站点工作人员检查，此站点内部局域网畅通，说明问题出在总部与该站点之间的网络互连设备或线路上。

接下来，我们把排查重点放在网络互连设备和线路上。登录到总部路由器，检查该站点对应端口的参数（包括网间网地址、封装协议、以及路由协议等），未发现问题；在总部机房的 2M 配线架对应线路上打环（如图 2 所示），在路由器输入命令 `show ip interface serialX brief`，显示：`serialX is up, line protocol is up (looped)`。总部机房 2M 配线架到路由器对应端口的线路形成环路，

说明路由器对应的端口硬件无故障；2M 配线架到路由器之间的线路也没有问题。由此判断故障不在总部机房。

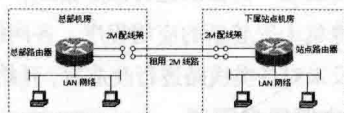


图 2 总部机房 2M 线路打环示意图

总部机房 2M 配线架拆环恢复后，与该站点协同，在其 2M 配线架打环（如图 3 所示），总部路由器仍然显示形成环路，说明租用的 2M 线路及两个机房的光端机工作正常。推断故障部位应该在该站点 2M 配线架以内。抢修小组决定到现场进行排查。

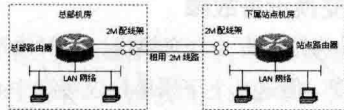


图 3 下属站点机房 2M 线路打环示意图

到达现场后，发现 2M 配线架对内打环时，路由器 LINK REM SYNC LOSS（E1 远端同步丢失告警）红灯亮，说明并未形成环路。自此，断定故障就在 2M 配线架与路由器之间的同轴电缆或本地路由器上。

我们先检查了 2M 同轴电缆的四个接头，焊点牢固并未发现异常。然后，把怀疑重点放在路由器上。反复检查了路由器参数，确认设置正确。是不是路由器硬件故障？更换备份路由器，重新配置参数，故障仍未解决。此时，抢修小组有些茫然。

故障排除

待冷静下来，回顾了整个排查过程，可以确定总部路由器和光端机正常，租用电信公司的 2M 线路也没有问题，该站点也更换了新的路由器。那么，故障可能就在该站点 2M 配线架到路由器之间的同轴电缆上。于是，在 2M 配线架对内打环的情况下，用万用表欧姆档测量，

发现同轴电缆屏蔽网形成回路，但芯线开路。

从电缆槽中取出两根同轴电缆仔细检查，终于发现其中一根有一处被压扁。剥开线缆，发现芯线已被压断，屏蔽网未被压断。我们推测，在机房搬迁过程中人多手杂，这根 75-2 细同轴电缆受到重物挤压所致，而人们恰恰又没注意到这一点，为后续工作留下了隐患。重新制作了一根同轴电缆，连接后故障排除。

故障分析

抢修小组在整个故障排查过程中，采用分段排查法，逐步将故障范围缩小。通过打环，将故障部位压缩在该站点 2M 配线架以内的线路或设备上。故障排查总体思路是对的，采取的排查方法也是恰当的。但是，在观察到该站点对内打环，路由器 LINK REM SYNC LOSS（E1 远端同步丢失告警）红灯亮后，凭借惯性思维，觉得电

缆中间不会出问题，检查了线缆接头后，转去怀疑路由器，而与真正的故障点擦肩而过。

如果当时对同轴电缆认真排查，就会及早发现故障部位，缩短故障排查时间。值得庆幸的是，虽然走了一点弯路，但是经过冷静的思考后，终于定位了故障点，故障得以排除。

经验总结

网络连通性发生问题时，故障原因都不尽相同。但通常可归纳为三类原因引起，即：设备硬件故障、软件参数设置故障、线路故障。遇到故障，不要慌乱，只要思路清晰、方法得当，就能快速定位并排除故障。

机房搬迁工作，头绪多、人手杂。人们往往比较重视各类设备的安全，而忽视了线缆的安全。本案例告诫我们，在机房搬迁过程中线缆安全也同样重要。



无线路由引发网络故障

湖南 廖滢

网络环境

单位网络使用三层结构，用户电脑及室内交换机等接入楼层弱电井汇聚层交换机，再由汇聚层交换机接入机房核心三层交换机。核心交换机上接有新闻采编系统等业务系统服务器，防火墙、负载均衡等设备。采用华为 eSight 网管系统，可以对汇聚层及核心网络交换机等可网管设备进行管理。

单位网络的设计原本并未考虑无线上网的需求，但随着无线上网越来越普及，特别是近年来单位开发了掌上长沙手机新闻客户端 APP 后，用户对无线上网的需求越来越多。技术部在部分楼层增设了无线上网设备，但覆盖率不能完全满足用户要求，有时在重点部位应用户要求还需增设小型无线路由器。随着无线设备的增加，网络故障发生率也在悄悄增加。

故障现象

某日下午，多个部门先后反映多台电脑不能上网。到现场查看的同事发现，故障有如下共同点：故障电脑都连接在同一台室内小型交换机上，分布在不同楼层的不同部门。交换机上还连有其他已关机的电脑，并且这些已关机电脑网线灯闪烁，证明有数据在传输。将室内交换机上连接的已关机的电脑断电或开机，故障可以排除。

故障排查

技术部同事当天晚上加班时，对白天发生过故障的端口进行了监测，故障并未再现，但在凌晨仍有别的部门上晚班的同事反映，需共享的视频无法传递。第二天正好是周末，因单位上班的人数相对较少，技术部仅安排笔者一人上班，笔者密切监视网络，同时用 Wireshark

抓包工具在不同时间段抓包,也未见异常。登录 eSight 网管系统,对发生故障及未发生故障的室内交换机接入端口同时进行监测比对,发现发生故障的端口在故障当天带宽流出利用率及端口流出速率出都达到了本月峰值(如图 1 所示),未发生故障的端口带宽接收速率也达到了近期的峰值(如图 2 所示)。

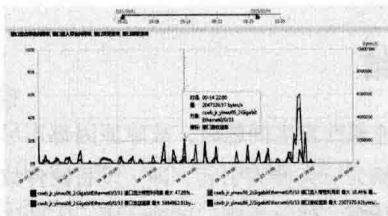


图 1 故障端口本月带宽利用率及端口速率 (包含输入输出) 监控图

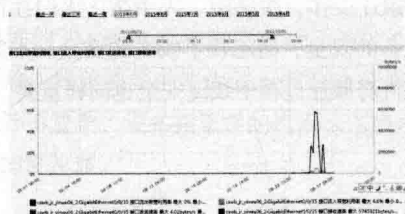


图2非故障端口本月带宽利用率及端口速率(包含输入输出)监控图

到底是什么原因导致故障当天数据量猛增呢?转眼快到下午 5 点了,由于晚上是出报时间,上网的人数渐渐多了起来。突然电话铃响了,夜班编辑中心有同事反映不能上网。赶到现场,在不能上网的电脑上安装 Wireshark 进行抓包分析,软件运行后几乎卡死,原来是有大量的 UDP 数据在网络中发送,造成抓包软件响应迟缓,据软件统计,76 秒内有 150 多万条,且数据包的大小都一致,显然是非正常的通讯数据包(如图 3 所示)。

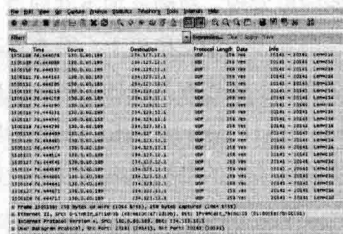


图 3 故障电脑 Wirshark 软件数据包抓取界面

终于找到原因了，于是根据发包的源 IP 地址在设备管理系统里查找相应设备，根据登记的数据显示，是夜班编辑中心的一台电脑。但是拔除这台正在使用的电脑网线后，大量发包现象仍存在。仔细核对 Wireshark 中抓到的源 MAC 地址和找到的电脑 MAC，发现不对应，仅 IP 是相同的。再次在设备管理系统里通过源 MAC 查

找，但没有找到设备。为加快查找速度，通知同事共同查找。同事赶到后也没找到此 MAC 地址的登记，面对分布在不同楼层的几百台网络接入设备没有了头绪。

笔者决定，还是登录 cSight 网管设备来查找这台未知设备。因为只要设备接入了网络，其 MAC 地址、使用过的 IP 及曾接入的交换机端口，在网管系统里应该都有记录。在网管系统里输入源 MAC 地址，这台设备曾使用的真实 IP 及接入的交换端口都显示出来。同事一看 IP，惊呼道：“这不是昨天下午我设置的一台无线路由的 IP 吗！”。原来，故障发生那天，有位用户需要手机上网查看掌上长沙的新闻客户端，于是向技术部申请安装无线路由器，正好是由同事设置安装这台新购的无线路由器。当时测试无线使用是正常，但没想到会引起网络故障。

故障排除

立即赶到安装故障路由的办公室，将设备拆下来，网络恢复正常。

第二天，同事又对此台路由器又进行了测试，发现只要接入集团局域网，立刻就会有大量 UDP 数据发送，此时对百兆网络的占用率超过 40%（影响较大），千兆网络占用率超过 4%（影响不明显），这就是为什么网络故障均发生在连入室内小型交换机，及需要大量传输数据的用户端的原因。再次确认了此台无线路由器是故障所在，并且重置路由器更换网络设置无效，只能更换设备。在更换此无线路由器后，又对网络进行了多天的监控，网络故障未再现，网络恢复了畅通。

经验总结

在无线应用越来越多的今天,各种无线设备的使用便利了用户,也增加了网络管理的难度。手机、笔记本、无线路由器等各设备的增加,对传统网络带来的各种安全问题是不可回避的。

首先，切记网络设备的登记，特别是无线路由器等入网设备的 MAC 地址及时登记，这是网络管理的基础资料。故障设备的定位一直是个难题，如果有详细的设备登记，在排查故障时将省时省力不少。

第二,要了解网络协议相关知识,善于借助网络分析管理工具。网络故障现象各式各样,有的可以根据现象判断原因,但情况复杂时仅根据现象是难以判断故障

原因的。这时就要借助专业的网络分析管理工具，并且了解一些网络传输协议的相关知识，学会使用分析管理工具对网络数据包进行相关统计分析。这次将开源软件 Wireshark 网络数据分析工具和集团现有的 eSight 网管系统结合使用，是快速诊断并排除故障的有效方法。

第三，密切关注单位业务的发展方向，当单位业务向无线发展时，或是用户无线上网的需求增加时，就应

根据业务的发展方向及用户的需求适时改变现有网络结构。重视无线局域网的建设，适时引入无线网络管理产品，排除网络安全隐患，避免网络的故障发生。如果将来上线移动采编系统，实现移动办公，对现有的无线局域网安全和性能将会要求更高。以业务为核心驱动信息化建设，是将来信息化建设发展的必然方向。

路由故障分析三例

福建泉州 李贵华 石海潜

故障现象一

最近，由于单位网络升级改造，单位与下级单位之间扩容为两条相同带宽的路由，一主一备分担网络负荷，提高网络通信的稳定性。下级单位报告说，升级改造后网络速度的确有了明显提高，但网速好了一段时间后就回到了升级改造前，上网速率非常慢，网络拥塞现象比较明显。

分析与排除：首先通过 `show ip route` 查看路由表，发现本级和下级单位之间只有一条主用信道的路由在用，而备用信道的路由没有启动。这就使得实际通信带宽减少了 50%，交换处理能力下降，网速降低。

而后输入命令 `show ip ospf neighbor`，通过查看 OSPF 配置，发现在该备用信道上，单位和分部之间并未建立邻居关系。尝试启用 OSPF 协议，其具体配置命令如下：

```
(global) router ospf 1
```

```
(router) network 互联网段 通配掩码 area 0
```

例如，本级单位与下级单位的互联网段是 10.10.11.1/29，则上行命令为：`(router) network 10.10.11.1 0.0.0.7 area 0`

执行命令后，显示双方邻居关系建立成功，两条信道通信正常，故障排除。

故障现象二

下级单位报告联不上网，网络联接不通。

分析与排除：首先观察本单位到下级单位的物理端口是否正常，如果不正常，可能的原因是：一是本级单位到下级单位的线路阻断，则处理线路问题。二是本单位到下级单位的端口损坏或者是下级单位的出口端口损坏，更换端口即可。

如果物理端口正常，则需要测试网络的连通性。登录路由器 Ping 下级单位路由器，如果不通，输入命令“tracert 目的地址”，出现“***”，说明该地址不可达，跟踪不到路由。笔者最后用 `show ip route` 命令查看故障网络的路由路径时，发现下挂用户的端口显示 `line up, line protocl down`，表明两个路由器之间物理链路是 Up 的，但协议是 Down 的。通过比对两端配置，确认网间网 IP 地址配置正确。再次输入命令 `show ip ospf neighbor`，发现 OSPF 协议未启动。

故障原因查找到了，排除方法也比较简单，按照故障一中的方法启动 OSPF 协议后，再 Ping 下级单位的路由器网关，网络测试通过，故障排除。

故障现象三

单位某部门报告说网络不通，通过现场查看发现无法 Ping 通路由器网关，但可以 Ping 通汇聚层交换机。

分析与排除：笔者首先排除了汇聚层以下可能导致

网络故障的因素，直接登录单位路由器查看日志信息，发现在互联线路质量不好的时间段，与该用户交换机直连的端口频繁出现 Up/Down 告警。图 1 为路由器的部分日志信息。

```
*Feb 9 10:42:26.435 ZZ: %LINK-3-UPDOWN: Interface
fastEthernet9/12, changed state to up
*Feb 9 10:42:27.015 ZZ: %LINK-3-UPDOWN: Interface
fastEthernet9/12, changed state to down
*Feb 9 10:42:26.435 ZZ: %LINK-SP-3-UPDOWN: Interface
fastEthernet9/12, changed state to up
*Feb 9 10:42:27.019 ZZ: %LINK-SP-3-UPDOWN: Interface
fastEthernet9/12, changed state to down
```

图 1 路由器的部分日志信息

很快，该端口变为 err-disable 状态，对应的日志信息如下：

```
*Feb 9 10:46:31.967 ZZ: %PM-SP-4-ERR DISABLE:
link-flap error detected on fastEthernet9/12, putting in err-
disable state
```

```
*Feb 9 10:46:32.147 ZZ: %PM-SP-STDBY-4-ERR
DISABLE: link-flap error detected on fastEthernet9/12,
putting in err-disable s
```

查阅技术资料，该款路由器的以太网端口反复出现告警后会造成网络不通。原因是该设备厂商为保证网络的可靠性，启用了保护功能：如在 10 秒钟内路由器的以太网端口反复出现 5 次以上 Up/Down 告警，路由器会因检测到端口出现 link-flap error 错误，而将端口置于 err-disable 状态。

针对这种情况，厂商也提供了相对应的自动恢复功能，只不过该功能默认关闭。输入命令“errdisable recovery cause Link-flap”，可以启动自动回复功能，提示设置自动恢复延时，默认为 300 秒，根据实际情况，设置自动恢复延时即可。

替换法解决存储问题

河北 王春海

故障现象

一台 IBM V3500 存储，有 2 个控制器，每个控制器具有 2 个 SAS 接口，通过 SAS 线连接到 3 台服务器。这个存储服务器在 Slot1、2、3、4、5、7、8、9、11、12 盘位安装 3.5 寸 600GB 的 SAS 磁盘。原来这个 IBM V3500 只有一个控制器，后来通过升级的方式，添加了第二个控制器，但添加控制器之后，第三个舱位（Slot 3）的磁盘出现黄色的报警，显示只有 Port 0 连接到了这个磁盘。

解决方案

对于上述故障，我们尝试了多种方法都没能解决，因为存储已经使用多年，有许多数据，另外，虽然提示有这个报警，但每个服务器都能连接、使用存储，数据存储显示也正常。

因为在 Slot 6、10 还有两个空闲的盘位，原来一直

是空着。后来想，可以在 Slot 6 或 10 盘位，添加相同的磁盘，将 Slot 3 的磁盘“替换”到 Slot 6 或 10，来解决这个问题。

故障处理过程

1. 在 Slot 6 与 10 插上相同型号的两个磁盘，将这两个磁盘设置为全局热备磁盘。
2. 右击 Slot 3，在弹出的快捷菜单中选择“Advanced → Fail”（如图 1 所示）。

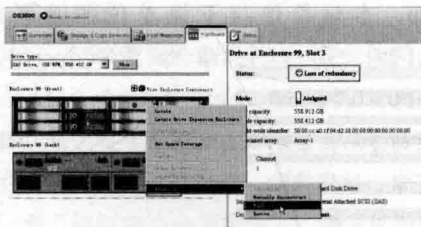


图 1 将磁盘标记为 Fail

3. 在弹出的“Confirm Fail Drive”对话框中，输入

- Yes，然后单击“OK”按钮。
- 将 Slot 3 标记为 Fail 后，全局热备磁盘将生效。在此 Slot 10 舱位的磁盘开始同步数据，Slot 10 加入阵列。
 - 此时 Slot 3 状态为失败。
 - 在查看阵列，涉及到 Slot 3 所在阵列 Array-1 阵列到数据正在同步（如图 2 所示）。



图 2 阵列数据正在同步

- 在阵列中更换物理硬盘或有失效硬盘时，逻辑磁盘状态为“Degraded”，在磁盘同步完成状态为

- “Optional”。
- 返回到“Hardware”选项卡，右击 Slot 3，在弹出的快捷菜单中选择“Replace”。
 - 在弹出的对话框中，显示将把失败的磁盘从 Slot 3 替换到 Slot 10 的位置，单击“Replace Drive”按钮（如图 3 所示）。

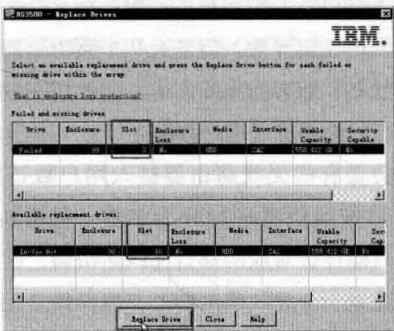


图 3 替换驱动器

- 在弹出的对话框中单击“OK”按钮。
- 返回到控制台界面，Slot 10 的状态已经正常。
- Slot 3 模式为未分配。至此整个替换完成。

揭秘无线同频干扰

天津 闻婷婷

故障现象

某工作日下午，笔者接到单位办公室同事的电话，反映会议室使用无线接入特别缓慢，亟待解决。笔者赶到现场后，发现会议室正在进行一项集体培训，参加人数有八十多人。经过了解，这次培训是针对业务人员的一次专项培训，目的是让业务人员尽快熟悉新上线的业务系统，培训过程中需要业务人员对应用系统进行实际操作，所以需要参加培训的业务人员自带笔记本、平板电脑或者智能手机接入公司内网，然后进行实际操作训练。

虽然会议室并未部署无线网络，但会议室分布着多个可供有线接入的墙点，由于公司并未实施严格的准入控制策略，所以只需要将设备或者终端接入墙点，采取

“自动获取 IP 地址”的模式，即可获得内网 DHCP 服务器分配的 IP 地址信息，顺利接入内网。

为满足用户使用无线的需求，办公室同事就自行部署了十个某品牌的家用无线路由器，这十个无线路由器均匀分布在会议室的周围，每个无线路由器的 SSID 均不一样，但是供用户接入的 WPA 密码都一致。培训开始前，同事还对这十个无线路由器单独进行了测试，确定每个无线路由器都正常工作，但是培训开始后，用户普遍反映无线网络缓慢，有时根本就无法打开业务系统，同事对所有无线路由器进行了重启操作，仍然无济于事。

故障分析

针对这一故障现象，首先需要排查是系统问题还是

网络问题。联系系统管理人员，检查了系统及服务器的状态，排除了系统的问题，这样问题就定位到网络上。经过笔者检查，其他办公地点的用户使用网络均正常，说明公司的骨干网络和接入网络并无异常，问题肯定就出现在会议室的无线网络上。

我们采取“先硬件后软件”的故障排查方法，首先检查了无线路由器的物理状态，包括指示灯、管理后台等，均未发现任何异常，但是有几个路由器属于“忙闲不均”的状态，即有的无线路由器接入用户数达到二十以上，但有的设备接入用户数极少。

会不会是有些无线路由器接入用户数过多导致的呢？将用户按照位置平均分为十组，每组 8-10 个人，每组用户只能连接对应的那台无线路由器，这样就将用户平均分配到十个无线路由器上，确保每个无线路由器负载均衡。但是这样分配完之后，上网速度仍然异常缓慢，在笔记本上使用 Ping 命令对无线路由器进行测试，丢包率达到 40% 以上。但是笔记本通过网线接入无线路由器的 LAN 口，采取有线上网的方式，则一切正常。

通过上述测试，排除了无线路由器负载过重的原因，那么只剩下一个可能性，那就是无线同频干扰的问题。笔者登录无线路由器后台管理页面，发现这些无线路由器均属于双频设备，即同时支持 2.4GHz 和 5GHz 频段进行无线通信，而系统默认的频段是 2.4GHz，这也是这些无线路由器正在工作的频段。为了证实会议室内这些无线路由器间确实存在同频干扰，笔者使用了一款名字为 inSSIDer 的无线网络检测软件，这款软件完全免费，可以很方便在网下载安装使用，inSSIDer 能够对附近的无线网络信号源进行检测，收集每个无线网络的详细信息，包括无线路由器的 MAC 地址、SSID、当前所使用的信道、安全类型、信号强度、网速等，同时还能够对无线网络的质量及同频干扰问题进行分析，提供故障排查的依据。下面结合 inSSIDer 对 cosbulk-371 这个 SSID 的检测结果进行介绍（如图 1 所示）。

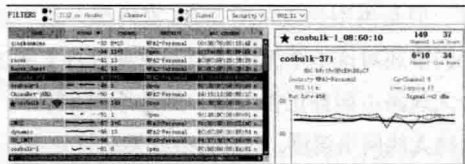


图 1 inSSIDer 检测结果图

从图 1 可以看出，左边框中详细列出了当前每个 SSID 的相关信息，可以看出 cosbulk-371 这个 SSID 目前工作在 2.4GHz 频段下，当前信号强度为 -42dBm，所

使用的信道为 6 和 10，采用 WPA2-Personal 安全技术，MAC 地址为 D8 :15 :0D :E9 :B8 :C7，采用的是 802.11n 无线通信协议；右边框中还能看到该无线网络的质量，着重需要关注 Co-Channel、Overlapping 和 Signal 三个参数的数值，Co-Channel 是指与该 SSID 使用相同信道的其他无线网络信号源的数目，Overlapping 是指与该 SSID 所使用信道频率上有重叠的其他无线网络信号源的数目，signal 是用来评估该 SSID 信号强弱的指标；其中 Co-Channel 和 Overlapping 两个参数值越高，表明该 SSID 遭遇的同频干扰越大；signal 参数值越高，越接近于 0，表明信号强度越高。

从图 1 可以看出，cosbulk-371 这个 SSID 的信号强度较高，但是遭遇的同频干扰比较严重，提供的无线网络不太稳定。

我们采用 inSSIDer 对会议室的无线网络进行检测后发现，基本所有 SSID 均工作在 6 和 10 频段，导致 Co-Channel 和 Overlapping 两个参数值都非常高，说明会议室内的无线同频干扰非常严重，这种情况肯定会导致用户上网极度不稳定。

故障排除

相对狭小的会议室空间内放置了相对多的工作在重叠信道的无线路由器，这些因素使得设备发生同频干扰的可能性大大增加，必须将这些无线路由器切换到不同的工作信道，尽最大可能避免同频干扰。2.4GHz 共存在十三个信道，但是这十三个信道并非完全独立，部分信道存在频率重叠的部分，所以为了避免干扰，一般会选取 1、6 和 11 这三个不重叠的信道进行无线部署。但是，会议室内有十个无线路由器，如果选用 2.4GHz 频段进行通信，不可避免地会有部分无线路由器存在同频干扰的问题，频宽窄、不重叠的信道少，这也是采用 2.4GHz 频段的固有缺点。

为了彻底解决同频干扰的问题，笔者决定采用 5GHz 频段进行通信。因为 802.11n 协议支持 5GHz 频段，而且该协议已经推广很多年了，属于非常成熟的主流无线通信协议，现有的笔记本、手机等无线智能终端和无线路由器基本都支持 5GHz 的频段。更重要的是，5GHz 频段划分了 24 个独立信道，每个信道不存在频率重叠的部分，这样就为无线网络提供了丰富的信道资源和更高的频宽，也有效避免了同频干扰的问题，只要将不同 SSID 固定在不同的信道，理论上就不会出现同频干扰

的问题。

登录各个无线路由器管理页面，将无线路由器的工作频段指定为 5GHz，并将十个无线路由器的工作信道分别设置为十个不同的信道，完成这些操作后，让用户重新接入对应的 SSID，无线网络立即恢复正常。随即使用 inSSIDer 软件检测会议室的无线网络质量，发现 Co-Channel 和 Overlapping 两个参数均为 0，说明会议室内完全不存在同频干扰，无线网络达到了最优状态。

经验总结

无线网络已经成为用户最为依赖的 IT 基础设施，

但是在企业内搭建一套稳定、安全的无线网络并不是一件简单的事情，首要解决的就是同频干扰的问题。传统的 2.4GHz 频段已经负重不堪，在某些干扰信号密集的区域，如果无线网络还使用 2.4GHz 频段，很容易发生同频干扰。所以，应该优先使用 5GHz 频段，合理分配信道，彻底根除同频干扰。

本文案例中所使用的家用无线路由器没有信道自动优化的功能，需要管理人员手动分配信道。现在市场上的主流商业无线方案，可以利用检测算法实现自动信道优化，减少同频干扰，有条件的单位可以尝试。

❖ 华为交换机互联出故障

▼ 辽宁 高大伟

随着国家电子设备国产化政策的实施，华为交换机作为网络互联必不可少的重要设备，其配置的正确性及其连通性对网络通信的可靠传输有至关重要的作用。本单位两个机房基于华为 57 系列交换机互联，但在具体配置时由于传统经验作祟，使得数据机房的网络无法连通。

故障现象

笔者单位近期进行了网络中心站和数据机房的改造建设，从电子设备国产化的角度考虑，为网络中心站和数据机房购置了华为交换机。网络中心站和数据机房连接关系如图 1 所示。

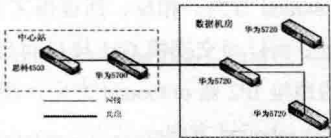


图 1 网络中心站和数据机房连接关系

其中，中心站华为 5700 交换机为 24 电口 +4 光口，数据机房华为 5720 为 48 电口 +4 光口，数据机房的三个交换机分别启用了 VLAN5、VLAN6、VLAN7，网关

都设在思科 4503 上。中心站的思科 4503 与华为 5700 通过网线 Trunk 连接，中心站华为 5700 与数据机房主华为 5720 通过光模块 Trunk 连接，数据机房主华为 5720 与其他两个交换机通过网线分别 Trunk 连接。在思科 4503 启用 OSPF 路由协议，其他交换机的默认路由指向思科 4503。设备安装配置完毕后，数据机房主华为 5720 互联的用户与中心站及其他机房都能连通，但数据机房其他两台华为 5720 互联的用户与中心站无法连通。

故障排查

既然数据机房主华为 5720 互联的用户网络正常，那么说明到中心站的链路没有问题。用 Console 口登录到主华为 5720 上，Ping 其他两台的管理地址正常，说明主华为 5720 与其他两台华为 5720 的链路是正常的。再用 Console 口登录到另外两台华为 5720，Ping VLAN5、VLAN6、VLAN7 的网关地址正常，验证了交换机到中心站没有问题。但用 Console 口登录 Ping 交换机互联的用户时，无法 Ping 通。由于用户计算机配置了三块网卡，起初笔者还以为是多块网卡的问题，但将其中的两块网

卡禁用后，依然无法 Ping 通。

在交换机上用 traceroute 排查，发现默认路由到了思科 4503 后，竟然没有返回的路由。难道是路由配置的问题？在数据机房的华为 5720 及中心站的华为 5700 启用 OSPF 协议，但令人失望的是故障还是没有解决。

故障排除

以往在中心站华为 5700 上也连过同型号的交换机，配置完成后没有问题，怎么到了数据机房会存在这样的问题呢？看来问题在华为 5720 的交换机上。登录华为 5720 上查看 VLAN 状态，奇怪的是一台交换机的 VLAN6 协议没有启用，另一台 VLAN7 竟然没有显示。为什么 VLAN6 协议没有启用呢？难道不仅与用户互联的华为 5720 要启用 VLAN6，而且主华为 5720 也要启用 VLAN6 吗？在主华为 5720 启用了 VLAN6、VLAN7，数据机房 VLAN6、VLAN7 的网络用户能与

中心站连通了。

故障分析

笔者初步分析，作为级联交换机，华为 5720 与华为 5700 的配置是不同的，主华为 5720 必须要将互联交换机的 VLAN 在本件交换机上启用，否则其他交换机的网络是不通的。而华为 5700 及思科交换机不存在这样的问题，只有配置成 Trunk 接口允许所有 VLAN 通过即可。

经验总结

华为交换机由于型号不同，软件运行的版本也不同，在配置时，一定注意不能按照使用老交换机的经验配置，否则就会遇到网络不通的故障。其次，在遇到问题时，要注意查看设备的技术资料，虽然资料基本上都是经典配置，但在解决实际问题时会有一定的帮助。

用流量统计追查丢包

福建泉州 王刚 叶永安 陈广辉 郑佳梅

遇到交换机丢包类故障问题，一般都需要抓包分析，而多数情况因现场条件受限导致抓包不易实施。笔者通过交换机流量统计功能，可以快速定位产生丢包故障的交换机端口，可以大大提高处理故障的效率，有效提高网络管理人员对于丢包问题的定位效率，缩短问题解决时间，并根据丢包故障问题从二层和三层两个方面找出交换机丢包故障排除方法。

丢包故障点快速定位方法

对交换机而言，解决最困难的故障就是丢包类故障，引发交换机端口丢包的原因有很多，主要原因一般是由于物理故障、配置错误、病毒木马、物理连接不紧密等原因造成，丢包故障呈现时断时续、未中断速率慢等现象。可以使用交换机流量统计功能快速定位交换机丢包故障

端口或该端口的物理链路，因为流量统计抓取的是设备底层的统计，精确而快速，可有效分析数据丢包情况。

流量统计定位原理

如图 1 所示，假设从计算机 PC1 至计算机 PC2 丢包。针对交换机 Ge0 接口而言，报文源地址 IP1 至目的地址 IP2 是 inbound 方向，相反，回程报文 IP2 至 IP1 是 outbound 方向；而针对交换机 Ge1 接口而言，报文源地址 IP1 至目的地址 IP2 是 outbound 方向，相反，回程报文 IP2 至 IP1 是 inbound 方向。



图 1 流量路径示意图

在报文流转端口部署针对故障 IP 的入方向和出方向

的流量统计策略，可以判断数据包是丢在了链路上还是交换机转发异常导致丢包，通过交换机出入端口数据包的丢包数据和数据包转发数量比较，可以把故障范围精确到交换机端口或链路上。

流量统计部署方法

文中所有配置均以华为交换机 S7700 为例，如图 2 所示，根据流量转发路径，在流量的入接口和出接口分别配置流量统计。配置举例如下。



图 2 配置举例图

1. 配置流量统计策略

```
[S7700]acl number 3000
[S7700-acl-adv-3000]rule 0 permit icmp source
11.11.11.11 0 destination 22.22.22.22 0
[S7700-acl-adv-3000]rule 5 permit icmp source
22.22.22.22 0 destination 11.11.11.11 0
[S7700-acl-adv-3000]quit
[S7700]traffic classifier huawei
[S7700-classifier-huawei]if-match acl 3000
[S7700-classifier-huawei]quit
[S7700]traffic behavior huawei
[S7700-behavior-huawei]statistic enable
[S7700-behavior-huawei]quit
[S7700]traffic policy huawei
[S7700-trafficpolicy-huawei]classifier huawei behavior
huawei
```

2. 在 VLAN 或端口视图下应用策略

```
[S7700]interface GigabitEthernet 0/0/1
[S7700-GigabitEthernet0/0/1]traffic-policy huawei
inbound
[S7700-GigabitEthernet0/0/1]traffic-policy huawei
outbound
[S7700] interface GigabitEthernet 0/0/2
[S7700-GigabitEthernet0/0/2]traffic-policy huawei
inbound
[S7700-GigabitEthernet0/0/2]traffic-policy huawei
outbound
```

3. 查看流量统计结果命令

```
[S7700-GigabitEthernet0/0/1]display traffic policy
statistics interface GigabitEthernet 0/0/1 inbound
[S7700-GigabitEthernet0/0/1]display traffic policy
statistics interface GigabitEthernet 0/0/1 outbound
```

4. 清空流量统计结果命令

```
<S7700>reset traffic policy statistics interface
GigabitEthernet 0/0/1 inbound
<S7700>reset traffic policy statistics interface
GigabitEthernet 0/0/1 outbound
<S7700>reset traffic policy statistics interface
GigabitEthernet 0/0/2 inbound
<S7700>reset traffic policy statistics interface
GigabitEthernet 0/0/2 outbound
```

事例中，通过查看流量统计结果，可以很快定位丢包故障交换机端口或链路。

二层丢包故障排除

在找到交换机丢包故障端口或链路后，可按下列步骤排除二层丢包故障。

1. 检查接口与链路

丢包类故障，最常见的故障一般都是由于接口或接线连接不紧密造成的，对故障接口或链路的连接接口和连接线进行检查和紧固，主要查看接口是否连接紧密，连接线是否破损等。此外，进入交换机的配置模式，使用 display interface GigabitEthernet X/X/X (X/X/X 为交换机端口号) 检查出入端口状态、速率、双工模式是否正确，相互连接的两个设备的端口工作模式必须完全一致，且链路无 CRC 错误报文计数等。

2. 检查交换机端口工作状态是否正常

一般交换机都会使用 STP、RSTP、MSTP、RRPP 等协议，在这些协议发挥作用时，可能会造成有的端口处于阻塞或转发状态，当两种状态互相转换时，会造成数据包丢包。

3. 确保交换机配置正常

使用 display vlan X (X 为 VLAN 编号)，确认本交换机出入端口的 VLAN 相同，因二层转发只依赖于 VLAN+MAC。使用 display mac-address 命令，确认流量的目的 MAC 地址是否正确学习在出接口，同时需要关注是否存在 MAC 地址在多个端口产生漂移的情况。

4. 查看交换机出入端口是否存在拥塞

使用 `display interface GigabitEthernet X/X/X (X/X/X 为交换机端口号)` 命令查看问题端口信息。查看端口出方向是否存在 Discard 计数持续增加情况, 如果有则说明该接口存在流量突发拥塞情况。出现拥塞一般是数据流量超过交换机负荷或网络中有广播风暴。

三层丢包故障排除

在找到交换机丢包故障端口或链路后, 可按下列步骤排除三层丢包故障。

1. 按二层丢包故障的步骤先排除由二层故障引发的故障。
2. 查看源地址和目标地址之间的路由。如果源地址和目标地址之间无法 Ping 通或路由条目不稳定等原因, 也会造成数据包丢包。

使用 `display ip routing-table X.X.X.X (X.X.X.X 为目标 IP 地址)` 命令可以查看到目标 IP 地址的路由是否存在或正常。检查路由对应的下一跳是否可达, 可以 Ping 下一跳的 IP 地址来进行测试确认。如果 Ping 不通双方或一方处于交换机直联网段, 可以使用命令 `display arp | include X.X.X.X (X.X.X.X 为目标 IP 地址)` 检查这些设备的 ARP 是否已经在交换机上正确学习。

经验总结

遇到丢包问题可以使用流量统计的方法快速方便的定位故障设备端口所在, 相关端口的流量是否在合理范围内, 以及是否有连续的、错误吧统计增加情况, 可以大大加快处理问题的速度以及缩小故障范围。找到故障端口或链路后依据故障产生的可能原因逐一确认排除。



设备兼容性带来的故障

山东 何钰 徐涛

故障现象

近日陆续接到用户报修, 反映宽带拨号错误代码 691。登录宽带用户管理系统查看, 发现该系统无法登录。对该系统所在服务器进行 Ping 测试, 结果请求超时。登录到 Radius 的上联设备核心路由器上查看互联端口状态, 发现端口是 Down 的。在核心路由器连接 Radius 的端口处, 发现了两者互联端口的状态指示灯不亮。将核心路由器光转电模块的网线进行插拔, 指示灯瞬间开始闪烁, 业务恢复了正常。

故障分析

根据该故障我们进行了总结, Radius 作为宽带认证的主要设备, 在网络中起到了核心的作用, 它一旦出现故障, 势必会影响用户正常的拨号上网。结合目前的网络情况和 Radius 服务器的部署, 我们提出了两种解决方

案, 一是更换光转电模块, 并认真排查网线。第二种方案就是将现有设备间的网线互联更换成光路。第一种方案比较易行, 可以购买适合核心路由器使用的光转电模块, 但是按照设备互联的规范和通常做法, 需要光路互联, 即第二种方案, 是解决问题的根本有效的途径。

故障排除

按照第二种方案进行优化升级, 同时将原有单台 Radius 服务器扩容至服务器集群, 形成数据库备份, 这样多台服务器都要和核心路由器互联。办法是, 将 Radius 服务器集群连接到一台交换机上, 然后该交换机使用光口和核心路由器互联。接下来开始对设备进行配置, 核心路由器上的做的操作主要是将端口进行强制千兆全双工, 具体命令如下。

```
Interface gei-0/1/0/2
```

```
// 进入端口
negotiation negotiation-force
// 端口强制
Duplex duplex-full
// 定义端口全双工
Speed speed-1G
// 定义端口速率千兆
```

完成核心路由器上的配置后，汇聚交换机上的配置操作也是将端口强制，主要是保证设备间链路的正常，避免不同厂家设备互联带来的其他问题。设备通过光路连接好之后，我们对服务器集群进行长时间观察和 Ping 测试，均没有发现问题。这样，该故障在得到解决的基础

上并合理地进行了优化升级，从而保障了 Radius 的正常工作。

故障总结

上面通过故障现象，我们经过排查得知，服务器和核心路由器之间是使用电路互联，为了保障 Radius 的正常工作，首先建立了服务器集群，实现了数据库的双备份。同时，将服务器集群使用交换机汇聚后，通过光路和核心路由器互联，该操作的完成完全符合服务器热备的要求，以及网络设备间互联的规范性，最大程度上实现了 Radius 服务功能的正常稳定运行。

排查 High CPU 网络故障

河南 赵志伟

故障现象

最近在一次日常工作中，突然接到某台汇聚设备 Cisco 6506 短信告警。立刻远程登录该设备，运行 show processes cpu sorted，发现 CPU 利用率已经高达 99%，IP Input 进程占了 73%。正常情况下，该设备的 CPU 使用率都在 10% 以下。

故障排查

1. 执行 show interface 或 show interface summary，查看哪些端口有较多的流量转发，以及这些接口是使用何种转发机制。建议执行本步骤之前，先执行 clear counters，对计数进行清零，便于观察流量的增长情况。

笔者喜欢用 show interface summary，相对简洁易看(如图 1 所示)。这里重点关注 RXBS 和 RXPS 两个指标的值，分别是每秒端口输入流量和数据包数。笔者发现，24 号端口 RXPS 数为 34241，远远大于同类型端口。查看端口配置发现，该端口为级联端口，进入该端口 shutdown，CPU 使用率立刻恢复正常。

```
cy01-6506#show interfaces summary
*1: interface is up
INQ: pkts in input hold queue      IQD: pkts dropped from input queue
OQD: pkts in output hold queue     OQD: pkts dropped from output queue
RXBS: rx rate (bits/sec)           RXPS: rx rate (pkts/sec)
TXBS: tx rate (bits/sec)           TXPS: tx rate (pkts/sec)
TRTL: throttle count
+-----+-----+-----+-----+-----+-----+-----+-----+
Interface      INQ  IQD  OQD  RXBS  RXPS  TXBS  TXPS  TRTL
+-----+-----+-----+-----+-----+-----+-----+-----+
* GigabitEthernet1/24  0    0    0    0 26790000 34241 18595000 2262  0
```

图 1 用 show interface summary 查看端口流量

故障基本可以确定是该端口下联设备所导致，联系下联单位网管处理即可。本着更加负责任的态度，决定揪出最终的“凶手”。

2.show ip traffic 的输入，可以告诉我们是哪类流量增长最快，之后再检查一下这类流量是否需要上送 CPU 做进一步处理，就能得出大致结论，High CPU 问题是哪类流量导致的。

3. 执行 debug ip packet detail，更直接查看到底是什么样的报文上送到 CPU 出发 CPU High，在执行该命令之前，建议在配置模式下先执行 no logging console 和 no logging monitor。

执行完 debug ip packet detail 后 3 到 5 秒，立刻输入 undebug all 命令停止。

4. 使用 show logging 查看结果，笔者发现某网段下两台主机以每 2ms 的速度发源端口为 14001，目的地址为 255.255.255.255，目的端口随机的 UDP 广播包。通过查

询广播主机 MAC 地址对应的端口，正是第一步查到的 24 口，也验证了第一步的结果。

故障排除

找到“病根”问题自然好解决。有两种方法，第一种“简单粗暴法”，shutdown 端口，通知故障单位网管，下联设备所属单位网管找到问题主机解决后，再回复。我们采用第二种：做 ACL，只需要输入两条 deny udp any eq 14001 any, permit ip any any, 在故障端口 24 口 in 方向上应用。再次输入 show processes cpu 查看，恢复正常。

经验总结

在 IOS 中我们把 SW process 叫做 IP Input 进程，简而言之就是数据报文没有被硬件 switching cache 或者 CEF 处理，而是 punt 到 CPU 去做进一步的处理。

在我们日常网络运维中，处理 High CPU 问题，除了采用我们上面的方法外，还可以依据实际情况用以下方式解决：如果您经验丰富去现场又方便，可以用 Sniffer 或 Wireshark 进行抓包；如果网络基础薄弱可以采取依次 shutdown 端口等同于现场依次拔网线，观察 CPU 的占用情况，从而发现故障端口。

配置失误导致监控异常

福建泉州 王刚 陈晓亮 叶永安 郑佳梅 陈瑜明

故障现象

单位建有视频监控系统，各监控终端经光缆连接至网络中心的网络硬盘录相机，将硬盘录相机的网口接入现有网络。监控值班中心使用网页浏览方式远程可以查看各监控终端信号，并将各监控终端信号投影至监控中心的各监控屏幕。

一天，监控中心值班人员向笔者反映，部分监控画面出现蓝屏、闪断现象，并且所有的监控屏幕都出现了很多横波干扰纹，特别是输出至新建 LED 高清背投屏幕横波干扰纹尤其明显。经了解，监控中心原有空间比较狭小，因任务需要，对原有空间进行了扩展，对现有网络进行了重新规划和新布设了部分线路，新增了几台交换机，加装了几台电视机和 1 块 LED 高清背投屏幕。为了确保新建 LED 高清背投屏幕工作良好，新敷设了 1 条专用地线。故障产生时，各设备已经安装完毕，其他施工内容也已基本结束，在调试设备时出现这些故障现象。

故障排除

1. 监控屏幕蓝屏的故障排除

(1) 施工单位技术人员对新布设的网络线路、视音

频线路、强电线路等进行了检测、梳理。因原有线路未拆除、新旧线路有部分重合，极有可能产生环路。对老旧线路进行了梳理，没有发现线路短路、断路和环路现象。强电和弱电线路走线均按技术要求，不会出现造成电磁互相干扰的情况，排除线路因素。

(2) 对原有线路和现有线路进行了对比，发现弱电方面除新增加了几台 TP-LINK 交换机外，整个网络拓扑没有发生大的变化。强电方面新增了几台电视机、1 台 LED 高清背投屏幕和新敷设了 1 条专用地线，看来问题就出现在新增设备上。

(3) 进一步整理发现，出现蓝屏屏幕所使用的计算机网口均连接使用了新增的 TP-LINK 交换机，将部分蓝屏屏幕的计算机网口连接至旧华为 S5700 交换机，直接跳过新增 TP-LINK 交换机后，发现计算机工作恢复正常，蓝屏故障消失。由此判断，故障的出现肯定和新增的 TP-LINK 交换机有关。对新增的 TP-LINK 交换机进行了测试，发现其工作正常，看来有必要进行抓包分析。

(4) 对新增 TP-LINK 交换机各外连接口的网络流量进行了监控和抓包，发现 TP-LINK 交换机会发送大量的 TCN BPDU 数据包，在华为 S5700 交换机中出现了大量告警信息。通过告警信息分析，应该是由 STP 震荡原因

造成，遂在华为 S5700 交换机上使用 `display stp tc-bpdu statistics` 命令，对交换机上的 STP 信息进行了统计，发现在其中两个交换机的端口上接收到特别多的 TCN BPDU 报文，而这两个端口均连接了新增的 TP-LINK 交换机。

(5) 使用相应命令分别查看了华为 S5700 交换机和新增 TP-LINK 交换机的配置，发现 S5700 交换机开启了 STP 协议，新增 TP-LINK 交换机默认也开启了 STP 协议。原有华为 S5700 交换机的默认根桥为网络中心的 1 台华为交换机，而原有网络选取根桥的方法采用了默认的根桥选取方法，网络中心的该台华为交换机 MAC 地址最小，当新增的 TP-LINK 交换机加入网络后，其 MAC 地址比作为根桥的华为交换机更小，新增的 TP-LINK 交换机会使用新增的 TP-LINK 交换机作为根桥，而原有的华为交换机还继续使用原有根桥，当一个网络中的不同设备使用不同的根桥时，就造成了 STP 工作震荡，从而引发网络工作异常。

(6) 对原有作为根桥的华为交换机进行配置，直接设置其为根桥，其他所有的交换机采用默认即可，对所有的交换机进行重启，所有监控蓝屏的计算机均恢复正常。另外，还可以采取另一种方法，即关闭新增交换机的 STP 功能。但不提倡使用这种方法，因为这种方法治标不治本，当在新增 TP-LINK 交换机产生环路时，无法及时发现和排除故障。

2. 横波干扰纹故障排除

(1) 监控中心原有电视墙和新增 LED 高清背投屏幕出现横波干扰纹，一般都是由强弱电线路或大功率用电设备的电磁辐射干扰造成的。使用辐射检测仪对所有的强电线路、计算机、交换机、新增 LED 高清背投屏幕周边的电磁辐射进行了检测，发现电磁辐射均在国家标准范围内，未发现异常。

(2) 进一步分析，发现横波干扰纹的出现有可能是由新敷设的地线引发，因新地线只服务于 LED 高清背投屏幕，在使用辐射检测仪检测所有辐射强度都在正常范围后，笔者判断极有可能是 LED 高清背投屏幕连接的新地线存在问题。

(3) 监控中心有 1 台 UPS 电源供电和 2 条地线。所有的供电由 UPS 电源供给，应该说电路相当稳定，可以很好地过滤各种谐波和干扰波，除 LED 高清背投屏幕使用了新地线外，其他设备的接入了旧地线。将 LED 高清背投屏幕接入旧地线后，所有的横波干扰纹消失，看来是新敷设的地线存在问题。对新敷设的地线进行了检测，发现其电阻小于 2 欧姆，接地良好，不存在故障，检查

了各连接接头后，又将 LED 高清背投屏幕连接至新地线，又产生了横波干扰纹。

(4) 将所有的设备地线均接入新敷设的地线后，所有的横波干扰纹也消失了。看来问题出现在新旧地线之间，使用万用表对新旧地线的压差进行检测，发现新旧地线之间存在 6 伏左右的压差。而横波干扰纹的产生就是新旧地线之间的这个 6 伏压差造成的，后将新旧地线进行了焊接，然后将所有的设备连接至地线，横波干扰纹消失，故障排除成功。

故障原因分析

蓝屏的产生，分析其原因是华为交换机和新增 TP-LINK 交换机 STP 协议选举根桥的工作方式不同造成的。作为华为交换机，默认是不启用 STP 协议的，在华为交换机启用了 STP 协议并且所有交换机工作稳定后，会按照默认方法选举根桥。为提高网络的稳定性，即使有新的华为交换机加入到网络中，也不会重新选举根桥。但如果所有的交换机重启后，则会按照默认的方式重新选举根桥。而 TP-LINK 交换机则不同，当的新入交换机接入后，如果新入交换机的 MAC 地址小于作为根桥交换机的 MAC 地址，就会造成重新选举根桥。

横波干扰纹的产生，分析其原因是当所有的设备连接至同一个 UPS 电源后，却使用了不同的地线，就会造成不同地线之间出现一个压差，而这个压差的出现就会产生谐波，从而形成横波干扰纹。

经验总结

华为交换机和 TP-LINK 交换机的根桥选举方法均使用 STP 算法，其根桥选举的默认方法是采取谁 MAC 地址最小谁为根桥，该方法一般适用于网络规模不大的网络。在网络规模较大时，一般会指定根桥，通过设置优先级的方法指定根桥，而作为根桥的交换机一般要求性能最好。当不同交换机同时接入网络时，一定要使用双方都支持的网络协议，在使用时，一定要区别这些网络协议在不同交换机上的使用方法的的不同，使用方法如果不正确，极易造成网络故障。

在一个网络机房内所有的防静电地线最好能使用同一个地线，当使用不同的地线时，很可能造成不同设备之间出现压差，而压差会造成设备之间出现干扰，程度轻一点会造成设备工作异常，严重时会造成设备损坏和减少使用寿命。

HP 小型机数据库故障处理

湖南常德 章昌军

单位有 2004 年购置的 HP 小型机数据库系统，操作系统为 HP-UX，数据库为 Oracle 9i，分别由 CDCZ 和 CDFS 两台 HP 小型机和 HP1000 磁盘柜组成双机共享磁盘柜系统。该系统承载着单位的三个核心业务系统。在 12 年的运行过程中，基本没有发生过问题。由于 HP 小型机系统对温度的要求较高，温度在 30℃ 以上就会产生宕机，所以单位中心机房的运行环境保障非常得力，环境温度始终保持在 20℃ -25℃ 之间。

故障现象

三个业务系统均不能正常访问，无法单独连接业务系统的核心数据库，确认为核心数据库问题。通过查看数据库服务状态，主机已经无法正常显示出数据库状态。

1. 经查看数据库日志，发现 CDCZ 主机上数据库 alert_cdcz.log 日志内显示，有错误产生，根据日志查看错误日志内容，主要如下：

(1) oracle/9.2/rdbms/log/cdcz_ora_9286.trc: ORA-07445: 出现异常：核心转储 [kollalo () +208] [SIGSEGV] [Invalid permissions for mapped object] [0x00000000] Tue Jul 26 09:25:32 2016 Errors in file

(2) /oracle/9.2/rdbms/log/cdcz_ora_25059.trc: ORA-04030: 在尝试分配 8528 字节 (pga heap, ksm stack) 时进程内存不足 ORA-04030: 在尝试分配 32840 字节 (pga heap, ksm stack) 时进程内存不足 Tue Jul 26 10:57:31 2016 Errors in file /oracle/9.2/rdbms/log/cdcz_ora_26977.trc: ORA-04030: out of process memory when trying to allocate

(3) locat ASYNC_CONFIG 配置错误

2. 通过 top 命令查看到系统内存剩余为 50MB 左右，说明系统内存消耗过高，对数据库影响非常大。

3. 通过 swapinfo -atm 命令查看到系统对虚拟内存使用率非常高，导致数据库对用户的请求响应变慢。

4. 综合以上信息并在 Oracle 官方网站查询资料后初

步判断：

(1) ORA-07445 错误为 Oracle 数据库软件的 Bug，需要通过对数据库打补丁包来修正这个错误，也可以找出诱发这个错误的应用语句，通过优化语句避免触发这个错误的发生。

(2) ORA-04030 错误，为 CDCZ 这台主机内核参数设置问题，可以通过调整内核参数来修正这个错误，主机一共有大约 50 项可调整参数，因为这个错误不是时刻发生，经过调整后的效果还需要观察。ASYNC_CONFIG，也是由于这个错误引起的。

故障处理及分析

CDCZ 主机因为数据库已经导致宕机，主机速度非常慢，故将这台主机操作系统重新启动，启动后没有加载数据库，剩余内存量为 6.9GB。

CDFS 主机也有部分内存泄漏，故也将这台主机重新启动，启动后剩余内存 6.9GB，启动数据库后剩余内存 3GB。

使用命令：cmruncl -fv 重新启动群集，数据库正常启动，应用恢复正常。

1. 将两台数据库主机重新启动后，加载 Oracle 数据库服务，数据库运行正常，同时三个业务系统也恢复正常。

2. 目前，Oracle 数据库服务加载在 CDCZ 主机上，数据库启动完毕后剩余内存为 3GB 左右，启动完毕等各项业务均连接至数据库，内存骤减至 1GB 左右，经查为三个业务系统中的一个业务消耗了大量内存和连接。

3. 本次调整了 CDCZ 主机上部分内核参数，调整后的效果还需要进一步的观察，因为引起数据库宕机故障不是非常频繁的发生，所以观察需要一定的时间。同时根据故障现象，小型机内存运行已严重不足，计划在一个月内存将小型机主机内存扩充至 16GB。

4. 目前系统运行在 CDCZ 上，运行的状态如图 1 所示。

CLUSTER	STATUS			
cluster1	up			
NODE	STATUS	STATE		
cdc2	up	running		
PACKAGE	STATUS	STATE	AUTO_RUN	NODE
pkg1	up	running	enabled	cdc2
NODE	STATUS	STATE		
cdfs	up	running		

图 1 系统在 CDCZ 上运行状态

通过上面运行状态记录可以看到，目前这个 PKG1 显示 enabled 是允许切换的。如果发生切换，会将数据库切换至主机 CDFS 上运行，状态如图 2 所示。

CLUSTER	STATUS			
cluster1	up			
NODE	STATUS	STATE		
cdc2	up	running		
cdfs	up	running		
PACKAGE	STATUS	STATE	AUTO_RUN	NODE
pkg1	up	running	disabled	cdfs

图 2 将数据库切换至主机 CDFS 上运行状况

通过上面运行状态记录可以看到，这个时候 PKG1 显示 disabled 是不允许切换的，需要手动将这个模式更改过来。操作如下：

- （1）以 root 用户登录到数据库运行的主机上。
- （2）用 cmviewcl 命令查看群集运行状态，如果

AUTO_RUN 状态为 disabled 则键入命令：cmmodpkg -e pkg1

（3）再次通过命令 cmviewcl 查看 AUTO_RUN 状态，确认状态为 enabled。

至此，整个小型机双机及数据库系统故障分析处理完毕。

经验总结

对于老的 HP 小型机数据库系统，由于购置的年代为 2004 年，受当时技术参数配置较低限制，尤其是内存，所以我们在该系统运行了一定的时间后，必须进行定期的技术维护和巡检处理，以便及时处理 CPU、内存运行在饱和状态故障，以及清理小型机系统和数据库日志等具体工作。必要时，需要增加设备的技术参数，如扩充内存等，熟练运用 HP 小型机的命令去查看运行状态、配置小型机的双机数据库系统以及处理故障。

防火墙故障排除案例

福建泉州 李贵华

防火墙是目前使用最为广泛的一种网络安全技术。它是不同网络或网络安全域之间信息的惟一出入口，能根据企业的安全政策控制（允许、拒绝、监测）出入网络的信息流，且本身具有较强的抗攻击能力。在构建安全网络环境的过程中，防火墙作为第一道安全防线，既可为内部网络提供必要的访问控制，又不会造成网络的瓶颈，并通过安全策略控制进出系统的数据，保护网络内部的关键资源。由此可见，对于连接到 Internet 的企业内部网络而言，选用防火墙是非常必要的。下面就结合笔者所用的天融信防火墙经常遇到的几种故障实例，来谈谈如何防护墙为维护。

实例一：客户机无法 Telnet 或 GUI 管理防火墙

遇客户机无法 Telnet 或 GUI 管理防火墙的情况，应首先检查防火墙登录控制中是否允许 Telnet 或 GUI 管理，若防火墙客户端列表中无 Telnet 或 GUI 管理，则增加防火墙 Telnet 或 GUI 管理登录客户。注意，正确选择登录客户的类型和正确填写该登录用户的 IP 地址范围。

其次，检查登录源主机的 IP 是否在设定的 IP 地址范围内，若不在设定范围内，则更改源主机的 IP 在设定的 IP 地址范围内。这一点特别要注意，很多防火墙维护人员为了方便，无限制地扩大了管理防火墙的 IP 地址范围，这样无疑给整个网络增加了新的安全隐患。然后，检查该防火墙是否为首次使用的新墙，如果是，则确认使用集中管理器（GUI 管理）登录防火墙的计算机应连接在

防火墙 ETH2 内网接口上。

最后，检查是否有相同用户名的用户已经登录防火墙，由于同名用户不允许在同一时间登录同一台防火墙，因此若同用户已经登录则应更改登录用户名，这个现象经常会遇到，特别是那种网页式的防火墙，虽然限制了用户的无响应时间，但在这个时间段内从别的计算机登录时则无法管理防火墙。

实例二：增加策略禁止某主机，该主机仍可通过防火墙

这种情况下首先应检查该主机与通信目标主机间的通信通道是否经过防火墙，如果不经过防火墙，再好的策略也无法起作用，也不能通过增加防火墙策略禁止该主机和目标主机间的通信。其次，检查是否已有策略允许该主机通过防火墙，若存在该许可策略则删除掉，大部分防火墙都遵循策略序号，即是从策略序号小的开始执行，一旦一条策略对某台主机生效后，后面针对该台主机的策略也是无法执行的，这一点要特别注意。最后，检查测试源主机是否配置双网卡以及多个 IP 地址，若是则禁用其中一个网卡。

实例三：IP 地址绑定未起作用

遇到这种情况时应该认真分析，其实 IP 地址绑定分为 IP 地址与 MAC 地址绑定和 IP 地址与用户绑定。当 IP 地址绑定未起作用时，检查绑定 IP 是否经过其他路由设备（路由器、三层交换机）才到达防火墙，由于通过路由设备后 IP 地址已被更改，原绑定 IP 地址失效，解决方法是更改路由设备为交换设备。

实例四：使用防火墙后原本可互相访问的主机无法通信

出现此问题主要有以下几个原因：

第一，主机所在的不同区域配置成 disable，应保证区域配置为 enable。

第二，通信双方主机在同一网段，防火墙设置的 VLAN 不包含主机所在的区域，应检查防火墙的 VLAN 设置，必须有一个 VLAN 包含主机所在的区域。

第三，通信双方主机不在同一网段，主机间没有路由设备，防火墙配置成透明模式，应在防火墙的两个接口上配置相应的 IP 地址，并把防火墙配置为路由模式。

第四，通信双方主机不在同一网段，主机间有路由设备，没有主机与路由设备在同一防火墙 VLAN 中，应保证其中一台主机与路由设备在同一个防火墙 VLAN 中。

第五，主机所在的区域访问策略中有禁止主机双方通信的策略，或主机所在区域的缺省访问权限是禁止的，应删除禁止访问策略，并保证缺省访问权限是允许的。

经验总结

在很多人眼里，防火墙无疑是“高大上”的，但作为网络安全运维人员角度来看，防火墙无疑就是“软件+硬件”的结合体，最重要的部分就是软件，软件水平的高低直接决定了防火墙的性能。默认情况下，所有的防火墙都是按拒绝所有的流量或允许所有的流量，因此在防火墙的配置中，首先要遵循的原则就是安全实用，从这个角度考虑，在防火墙的配置中需坚持以下三个原则。

一是简单实用原则。对防火墙环境设计来讲就是越简单越好。越简单的实现方式，越容易理解和使用。而且是设计越简单，越不容易出错，防火墙的安全功能越容易得到保证，管理也越可靠和简便。目前常用的防火墙在基本功能上都或多或少都增加了一些特殊功能，但这些增值功能并不是所有应用环境都需要，在配置时可针对具体环境进行配置，不必对每一功能都详细配置。

二是全面深入原则。单一的防御措施是难以保障系统安全的，只有采用全面的、多层次的深层防御战略体系才能实现系统的真正安全。在防火墙配置中，不要停留在几个表面的防火墙语句上，而应系统地看等整个网络的安全防护体系，尽量使各方面的配置相互加强，从深层次上防护整个系统。

三是内外兼顾原则。防火墙的一个特点是防外不防内，其实在现实的网络环境中，80% 以上的威胁都来自内部，所以要从根本上改变过去防外不防内的传统观念。对内部威胁可以采取其他安全措施，比如入侵检测、主机防护、漏洞扫描、病毒查杀。部署与上述内部防护手段一起联动的机制。



寻找无线信号异常根源

福建泉州 王刚 叶永安 陈晓亮 陈瑜明

当今,无线技术已经全面融入到我们的日常工作和生活之中,手机、平板、笔记本电脑已成为企业上网的标配,这些无线设备一般使用 2.4GHz 频段的无线信号上网。除此之外,还有无绳电话、蓝牙产品、无线键盘、无线鼠标以及无线耳机等无线设备也使用 2.4GHz 频段。当这些无线产品和企业无线路由器放在一起使用时,无线网络就会出现网速变慢、频繁掉线、甚至网络中断等现象,即出现了“同频率干扰”现象,会影响 Wifi 的传输速率,笔者就遇到了这种情况。

故障现象

有位同事说单位路由器信号不稳定,路由器连接运营商的速率是 50Mbps,路由器除有线连接计算机外,还有企业无线视频盒子和手机使用该路由器上网。当使用无线视频以 Wifi 方式连接路由器,上网看在线看视频时,经常会出现卡顿和中断现象,连接速率也很不稳定,速率快时可达 1.2Mbps,慢时仅为 7Kbps,手机以 Wifi 方式连接路由器后使用微信发送信息,数据会出现发送失败或提示无法正常连接服务器现象。

故障原因

造成路由器无法正常提供无线信号服务的原因有很多,常见的原因主要有以下几个方面。

1. 软件设置错误

很多企业路由器在购买后,很少会对其进行设置,大部分都是采用了默认设置,而很多路由器的默认都对无线信号进行了限速,当移动上网终端过多,每个终端分得到的带宽就会很少,造成无线信号不稳定。还有,当 WAN 口(至运营商的接口)实际使用的上下行流量接近线路的实际带宽时,也会出现上网慢的情况,在这种情况下可下,可检查 WAN 口设置的上下行带宽值是否正确,

过高过低都不好。

2. 环境问题

当路由器周边存在较大的干扰源时,就会出现信号不稳定。现在,企业路由器在使用时,其摆放位置都存在很大的随意性,很少考虑到路由器周边的电磁环境问题,但很多路由器极易受到周边其他电器的电磁干扰,特别是很多使用 2.4GHz 频段的无线设备,最易干扰路由器无线信号,比如:无线鼠标、无线键盘、无绳电话、蓝牙产品、无线耳机、微波炉、无线电视等,甚至电灯、空调、冰箱、洗衣机等电器都会影响路由器的无线信号。还有,当路由器摆放的位置不佳时,特别是摆放在离其他热源较近、太阳直射的地方或设备自己散热不良,长时间运行后,也会造成路由器工作不稳定。

3. 外连移动终端过多

一般企业路由器理论上可以外连 253 个终端,但实际上 100 ~ 200 元的企业路由器最多外连 15 台左右,而实际当 WAN 网速足够时,当外连移动上网终端超过 8 个时,其性能就会下降明显。当日常应用以观看在线视频为主时,外连移动上网终端数量应相应减少,必要时,可采用时间错开的方式上网。

4. 移动终端同路由器协议不相匹配

现在很多移动终端更新换代较快,但也有很多旧款的移动上网终端在使用路由器上网,而一般新购的路由器都采用了新的技术,但很多旧款移动上网终端都不能很好地支持路由器的最新协议,从而造成连接不稳定或频繁掉线。比如,现在很路由器都支持 IEEE 802.11n 协议,该协议在路由器的最直接的体现就是使用了 MIMO 技术(Multiple-Input Multiple-Output, 多人多出),很多旧款手机是不支持该协议和技术的。

5. 信道冲突

随着企业路由器的普及,路由器的数量急剧增加,邻里之间的路由器就会存在信道冲突的现象。当有多个路由器时,就会存在抢信道的问题,使用的信道相同时,

路由器之间信号发生干扰，路由器之间因干扰造成发射信号不正常，其对外服务的无线信号当然就会不稳定。

故障排除步骤

1. 使用 360 测网速工具对无线路由器外接网络速度进行检测，并对计算机和各移动终端查杀病毒。发现其上网速度正常。在计算机上打开视频网站，发现在线观看网上视频相当流畅，即使是高清视频或超清视频，都没有卡顿现象。由此也可以看出，路由器至运营商的线路正常。然后对计算机病毒库进行了升级，并对计算机和移动终端查杀了病毒，未发现病毒和木马。

2. 使用计算机登录无线路由器，发现对外连接的移动上网终端只有 1 台计算机、1 个无线视频盒子、3 部手机，各移动上网终端数量正常，没有未知移动终端使用本路由器。在计算机终端上分别 Ping 其他移动无线终端，发现到各终端的时延均在 200 ~ 1360ms 之间，且时延变化比较大，而且存在丢包现象。说明路由器至各移动无线终端的信号不是很稳定。在 3 部手机均关闭 Wifi 连接后，仅保留无线视频盒子连接路由器，发现在线播放视频仍存在卡顿和中断现象，即使在播放标清视频时仍会出现卡顿和中断现象，说明无线视频盒子出现了故障，也有可能是传输的无线信道出现了问题。

3. 将无线视频盒子有线连接至路由器，发现在线观看视频很流畅，没有出现卡顿和中断的现象。在计算机 Ping 无线视频盒子，发现时延均中 1ms 以内，丢包率为 0，说明无线视频盒子出现故障的可能性不大，即使出问题也是无线视频盒子无线发射和接收模块出现了问题。

4. 使用 360 相关工具对计算机外连的程序进行了检查，发现计算机内主要外连网络和消耗网络流量的进程主要有迅雷下载软件、迅雷视频软件、360 相关软件和其他一些视频播放软件，而这些软件并没有在使用。

5. 对周边的无线信号进行了扫描，发现有很多无线信号，有可能存在信道冲突。笔者手动对路由器信道进行了修改，发现无论是更换哪个信道，问题都没有很好地解决。看来，信道冲突的可能性也比较小，而用户移动上网终端都是比较新款的，支持最新的路由器协议和技术，不存在协议和技术不匹配的问题。

6. 对周边的环境进行了检查，发现路由器周边除了 1 台计算机、1 台交换机、1 个台灯外，其他的电器距离都比较远，不可能影响路由器正常工作，无线视频盒子旁边有一个电烤炉，而电烤炉也未开启。后发现该计算

机上连接了一个无线鼠标，看来，如果出现信号干扰问题就只有无线鼠标和台灯。在关闭鼠标电池开关后，问题仍然存在，而当关闭台灯后，发现无线信号一下子就恢复了正常。在计算机上 Ping 无线视频盒子，时延都在 30ms 左右，也没有出现掉包现象，故障得到排除。

后发现，这个台灯为卤素灯泡，查阅了相关资料后，才知道卤素灯泡会对无线信号进行干扰，这种情况还是第一次遇到。

经验总结

为保证路由器正常工作，笔者建议可以采取以下几项措施。

1. 企业路由器在摆放时，一定要远离干扰源，除了已知的电器设备外，还有很多未知的电器也会对路由器进行干扰，只是平时很少遇到罢了。随着无线技术的快速发展，2.4GHz 这个频段的拥挤现象还会加剧，对于 Wifi 用户而言，未来的“同频干扰”问题会更加严重。建议在购买企业路由器时，可以选购双频（2.4GHz+5GHz）的无线路由器，可有效避免路由器干扰问题。

2. 当路由器比较老旧时，特别是只支持 IEEE 802.11b/g 时，其只支持三个不重叠的传输信道，只有信道 3、6、11 和 13 是不冲突的，但使用信道 3 会干扰 1 和 6 信道，使用 9 信道会干扰 6 和 13 信道。所以，一般在发生路由器信道冲突时，可以手动选择 1、6、11 信道可有效避免冲突。

3. 可手动绑定各移动上网终端和对连接路由器的数量进行限制，避免其他非法用户使用路由器。在此基础上，可对各移动上网终端的网速进行设置或开启路由器的智能均衡功能。

4. 当 WAN 口的外连网速出现问题后，用户自己一般无法自己解决，可联系电信运营商进行上门排除故障。笔者碰到有用户自己计算机中了病毒后，上网速度很慢，用户以为是电信运营商的问题，打电话给电信运营商，而电信运营商可以远程对用户的 WAN 口的上网速率进行检测，如果用户 WAN 口网速正常，他们是不会上门服务的。

5. 当网络中存在病毒和木马时，除计算机可利用专业杀毒软件查杀病毒外，很难判断手机等移动上网终端是否存在病毒。遇到这种情况，可先移动上网终端和其他有线上网终端的业务，再直接观看路由器的信号灯其闪烁频率。如果闪烁比较快速，说明网络中存在病毒、木马或广播风暴的可能性比较大。

HP 服务器时间同步出 Bug

宁波 姚明友

网络环境

单位原先的两台 IBM3850 与两台 DS4800 由于使用年限过久，即将退居二线以外非重要的业务使用，新购了 4 台 HP DL5800 G9 及两套日立存储。暂且命名 4 台新设备为 A、B、C、D 机。装 Windows Server 2012 系统，再用系统自带的 HP-V 搭建虚拟化提供业务使用。单位有域控服务器（分主、备各一台），基本所有服务器包括 PC 机都加入此域被管理。这 4 台新购的服务器也加入此域。

整个架构搭建好后运行了一段时间基本正常，HP-V 上也创建了 2 台虚拟主机，各自装了操作系统，并在里面各自安装业务系统，命为业务 A、业务 B 系统。

故障现象

一天，业务 A、业务 B 系统出现问题，经描述了解到，操作者当时在软件上的操作记录时间记录到数据库时与北京时间不匹配，相差甚多，跟北京时间相差 8 小时左右。该问题很明显与服务器操作系统时间有关，因操作人员在软件上所操作的记录时间是统一调取服务器时间再记录到数据库，而且当时检查操作者 PC 电脑本地时间也是正确的，由此，怀疑到业务 A、业务 B 系统对应的服务器操作系统时间存在错误。

故障排查

登录业务 A、业务 B 的服务器上也发现，当时服务器的时间存在 8 小时的误差。

继续查找有关影响时间的操作系统日志，发现如图 1 所示信息，说明操作系统时间确实是有过更改记录，更改的时间范围为 8 小时。



图 1 业务 A 系统时间日志更改记录

经了解到，由于业务 A 与业务 B 的服务器为 HV-P 所创建的虚拟主机，而虚拟主机的时间同步依赖于承载虚拟机的物理机（当时买的 A、B、C、D 四台 HP DL5800 G9 服务器）系统时间。分别查看承载两台虚拟主机的物理机中系统日志，找到如图 2 及图 3 所示记录。



图 2 A 机系统日志

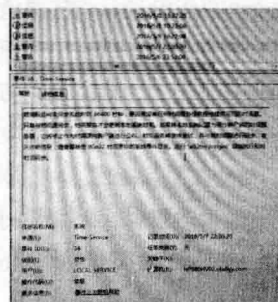


图 3 B 机系统日志

以上日志表明，由于两台物理主机长时间无法联系到原先的时间同步源（域控权威时间发布者）而被迫与本地 CMOS 时钟进行时间同步，但在 CMOS 同步时间后

系统时间被调慢了 8 小时。再去查看域控服务器时发现是关机状态。

经测试，这几台操作系统一旦与 CMOS 时钟进行同步，会立即造成操作系统时区错乱，继而发生系统时间被调慢了 8 小时的错误现象，判断是物理机的 BIOS 存在 Bug。

故障原因

1. 由于域控（权威时间发布源）服务器因硬件问题发生了宕机。
2. 在长时间无法与域控（权威时间发布源）进行联系后，物理主机会跟自身 CMOS 时钟同步造成系统时间发生错误。
3. 物理主机上的虚拟主机（业务 A，业务 B）数据库同步了物理主机的错误时间。
4. 最后造成在业务 A，业务 B 上发生的所有操作更新到数据库时的时间字段都被提前了 8 小时。

故障排除

1. 恢复域控服务器并重新制定可靠的时间发布源。
2. 修改物理主机操作系统上的注册表来解决操作系统与 CMOS 时间同步时的错误问题。修改命令下：

```
[HKEY_LOCAL_MACHINE\SYSTEM\
CurrentControlSet\Control\TimeZoneInformation]
"RealTimeIsUniversal"=dword:00000001
```

经验总结

现代信息技术越来越趋于专业化，软件一个方向，硬件一个方向，越专业后不可避免的问题就是兼容性。这次事件起因是时间发布源（主域控服务器）坏了，虽然有主备域控，但是时间发布源只能有一个。当时间发布源无法联系的时候，物理主机将于本机 CMOS 同步时间，恰巧 HP DL5800 G9 的 BIOS 存在 Bug，以至于同步时操作系统的时间调慢了 8 小时，导致记录到数据库的时间相继更改，发生了业务故障。在复杂的集成环境下分析问题时需耐心仔细，逻辑清晰才能慢慢找出源头并解决。

◆ 新换电脑为何无法上网

▼ 天津 贾娜 郁成军 余腾 王昆

笔者负责维护的单位办公自动化网络中一台电脑终端突然故障，因无修复价值，决定更换新电脑终端。这项工作不难且工作量也不大，只需按最初的网络规划设置新主机的相关信息，在接入交换机相应端口上对新主机 IP 地址、MAC 地址重新绑定后，新主机即可连接入网。然而，做这项工作时，因为忽视了交换机一条命令的作用，而阴差阳错地出了一些问题，导致该主机一直无法入网。

网络环境

笔者维护的办公自动化网络是一个局域网，各办公室的电脑终端均连接到接入交换机上，各接入交换机通

过汇聚交换机连接到核心交换机上。这样，就实现了办公电脑终端之间以及与服务服务器之间的连接。所有办公电脑终端一律禁用自动 IP 地址获取方式，而是采用人工指定 IP 地址的方式接入网络。为了确保网络安全，在接入交换机对应的端口上对电脑终端的 IP 地址、MAC 地址进行绑定，并对各部门的电脑终端进行了 VLAN 划分。在该办公自动化网络的建设过程中，使用了华为、H3C、Cisco 等几个品牌的交换机。

故障现象

一终户反映，他们有一台电脑故障，因使用年限较长，

市场上无法找到配件，已没有修复的价值，决定更换一台新电脑替代故障终端接入办公自动化网络。接到用户申告后，笔者对这台故障终端相关资料进行了梳理。它是通过办公楼内布置的网线连接到一台接入交换机的端口9上。这台接入交换机的型号为 Quidway S5352C-SI。该科室的另一台电脑终端则连接在这台接入交换机的端口8上。新电脑终端沿用故障电脑终端的网络线路及接入交换机的端口9。

明确任务后，根据现有的技术资料着手做这项工作。首先，在新电脑上设置原来为这台电脑规划的IP地址、子网掩码及默认网关等。

然后，通过 PuTTY 软件远程登录到这台接入交换机上，通过以下命令解除交换机上绑定的故障电脑相关信息：

```
# undo user-bind static ip-address XXX.XXX.XXX.XXX (故障电脑的IP地址) mac-address XXXX-XXXX-XXXX-XXXX (故障电脑的MAC地址) interface GigabitEthernet 0/0/9 vlan 2。
```

做完上述工作后，接上网线，通过命令 Ping 服务器地址，检查网络的连通性。结果表明网络不通。

故障排查

首先采用“分段法”，根据该科室另外一台电脑的状态，检查网络连通性，发现其对服务器网络线路畅通，而该科室两台电脑之间无法 Ping 通。这些说明从接入交换机、汇聚交换机、核心交换机到服务器这条网络线路正常，问题出在新电脑和接入交换机对应的端口之间。问题可能出在两个方面：一是软件参数配置不正确；二是物理层硬件有问题。

继续采用“分层法”来排查问题所在。根据现有的技术资料检查电脑网卡驱动安装、参数设置、接入交换机对应端口参数设置是否正确。经多人反复检查，没有发现问题。

继续检查物理层硬件。物理层硬件包括新电脑网卡、网线、接入交换机对应的端口。为了验证新电脑网卡是否有故障，我们将这台新电脑搬到维修间，用一台备用的交换机和一台笔记本电脑搭建了一个局域网。笔记本电脑IP地址设置与新电脑终端在同一网段，未对交换机端口进行绑定。接通网线后，新电脑终端和笔记本电脑之间能 Ping 通，说明新电脑网卡没有问题。

接下来检查网络线路。用网线测试仪检查网线，结

果表明网线正常。为了验证这根网线，我们把这台新电脑搬回科室，把备用的交换机和笔记本搬到接入交换机所在机房，再做与维修间同样的实验。设备加电连接后，笔记本电脑和新电脑终端之间能 Ping 通，说明墙内预置的这根网线没有问题。通过这根网线把新电脑主机连接到接入交换机的端口9上，仍然 Ping 不通服务器。

难道是接入交换机端口9出现故障了？我们决定用接入交换机的端口8来验证一下。端口8解除绑定后，新电脑终端的网线接到端口8上，仍然无法 Ping 通服务器。端口8重新绑定原参数，恢复原电脑终端的连接，结果网络畅通。在端口9上对新电脑参数绑定后，将新电脑终端连接到端口9上，发现新电脑终端居然能 Ping 通服务器，网络畅通。这让我们感到很茫然：接入交换机的端口绑定是对访问网络的电脑加以限定条件，网络反而畅通；解除绑定是取消限定条件，网络却不通？

故障排除

再回过头来，检查接入交换机端口9的配置信息：

```
interface GigabitEthernet 0/0/9
description lizhi
port link-type access
port default vlan 2
ntdp enable
ndp enable
bpdu enable
ip source check user-bind enable
```

看到“ip source check user-bind enable”这条命令后，忽然明白，虽然在接入交换机端口9上解除了对故障电脑终端的绑定，以为通过接入交换机这个端口访问网络就不再受限制。但是，由于这条命令的存在，接入交换机该端口对用户信息检查功能一直在起作用，导致接入交换机丢弃该端口报文，造成了新电脑终端无法入网的现象。

后来，我们通过实验验证：只有在解除接入交换机某端口对主机IP地址、MAC地址绑定的同时，通过命令 undo ip source check user-bind enable 解除接入交换机绑定检查功能，才算是彻底解除了通过接入交换机该端口访问网络的限制。

经验总结

在此之前也更换过电脑主机,但都没有出现类似现象。我们的做法是解除原主机 IP 地址、MAC 地址的绑定后,立即在接入交换机对应的端口上绑定新主机 IP 地址、MAC 地址,“ip source check user-bind enable”这条命令一直存在并起作用,主机入网没有问题。此次解除接入交换机的端口绑定后,我们觉得解除绑定限制条件更加便于调试网络,网络调通后再完成绑定工作,所以并

未急于绑定新主机的 IP 地址、MAC 地址,但也没有及时解除这条命令的作用,这才导致了新主机无法入网的假象。

排查这个故障持续了近一个星期,虽然走了一些弯路,但终于彻底理解了华为交换机端口绑定功能的实现机理,以及与其他品牌交换机的不同。这个事例告诫我们,作为网络管理人员,绝不能按惯性思维行事,在使用不同品牌的设备时,既要注意它们的相似之处,更要特别关注它们之间的区别,才能灵活高效地维护网络。

巧用 CNA 排除接线故障

广州 谈武强

网络结构

笔者所在单位出于安全考虑,组建了两套相互独立的局域网。综合化布线时为每个用户工作区(办公点)安置了两个网络接口,分属两个不同的局域网。这两个局域网是物理隔离的,不允许互访。每套局域网均为单核心、核心层—接入层的两层式结构,网络拓扑结构如图 1 所示。

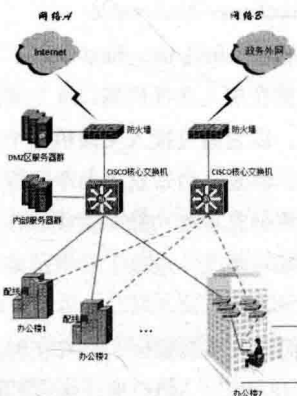


图 1 网络拓扑结构

局域网 A 核心层为 Cisco 6504-E 三层交换机,通过光纤连接 29 台 Cisco 2960 接入层交换机,划分了 35 个 VLAN,IP 规划为 192.168.0.0/24,网络出口区连接 Internet。局域网 B 核心层为 Cisco 6504-E 三层交换机,

通过光纤连接 23 台 Cisco 2960 接入层交换机,划分了 2 个 VLAN,IP 规划为 172.16.0.0/24,网络出口区连接政务外网。所有用户 PC 均为单网卡,同一时刻只能连接 A、B 网络中的一个,切换网络时需拔下网线后插入工作区另一接口。

局域网 A、B 均有各自的 DHCP 服务器,是在核心交换机上设置的,每个 VLAN 设一个 DHCP 服务器,所以网络 A 有 35 个 DHCP 服务器,网络 B 有 2 个 DHCP 服务器。

故障现象

前不久,部分用户反映无法正常上网。现场发现,用户明明连接的是局域网 A 的网口,却获得了局域网 B 的 IP 地址、子网掩码、网关和 DNS。Windows 命令行下用 ipconfig/renew 多次向 DHCP 服务器重新申请 IP,时而得到网络 B 的 IP,时而得到网络 A 的 IP。

故障分析

凭直觉判断,最可能的原因是网络 A 与网络 B 间发生了物理连接,使网络 A、B 组成了一个大的局域网,在这个大的局域网中同时存在 $35+2=37$ 个 DHCP 服务器,DHCP 服务器间是竞争关系,都具备向用户提供 IP

地址的能力。

用户网卡作为 DHCP Client，向网络中发送 DHCP Discover 广播报文，两台 DHCP 服务器均接收到 DHCP Discover 报文，然后向 DHCP Client 发送一个 DHCP Offer 报文。DHCP Client 只能处理其中的一个 DHCP Offer 报文，一般的原则是 DHCP Client 处理最先收到的 DHCP Offer 报文，然后发出一个广播的 DHCP Request 报文……

故障排查

网络 A 与网络 B 间发生了物理连接，该连接发生在核心层或接入层的可能性均存在。由于核心交换机放置在数据中心，由数据中心的网管人员管理维护，外人无法接触，基本上不可能发生核心层错误连线这种低级错误。经在数据中心现场勘查，没有发现两台核心层交换机间有任何连接，核心层互连的可能性被排除，那么互连只可能发生在接入层。

接入层互连点又存在两种可能，一在配线间，二在工作区。如果互连点在配线间，全单位共有十个弱电配线间，现场勘查找到互连点不需要太长时间。但如果互连点在工作区，全单位共有 500 多个工作区，1100 多个网络布线点（每工作区有网络 A、网络 B 接口各一个），且网络接口多数布置在办公桌后，需移动办公设备才能暴露网口和网线，排查的工作量非常大。那么有没有一种简单高效的方法来找到互连点呢？

对于 Cisco 的交换机，一种简单高效的方法是，使用 Cisco 公司为中小型企业提供的一款免费的、帮助网管员配置思科设备的工具——思科网络助手（CNA），优点是图形化、可自动产生网络拓扑，很直观。

到思科官网下载 CAN，最新版本为 6.3.0，安装过程很简单。运行 CNA，首先 Create community，输入要添加到管理组的交换机的 IP 或 IP 范围，输入交换机口令，软件即开始尝试与要管理的交换机建立通信，扫描到本组所有交换机后会形成并展示一个网络拓扑图，调整拓扑图的参数，使其显示设备链路接口 ID、设备名称信息。

我单位二层交换机 hostname 均按“建筑物名称首字母 + 配线间所在楼层 + F+D+ 本交换机在本配线间中的序号”的命名规则命名，如 Z2FD3 表示综合楼二楼政务外

网交换机中的第三台，MD2 表示门诊楼政务外网交换机中的第二台。目测右侧区域的拓扑图和左侧区域的交换机列表（放大后如图 2 所示），根据交换机的 hostname 发现问题。

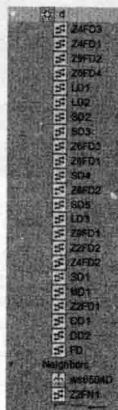


图 2 拓扑图左侧的交换机列表

图 2 字母 d 为创建出的 community 组名，表示政务外网组，其下方列出了本组所有二层交换机。Neighbors 表示与本组交换机有链路相连的其他交换机，这里列出了两台，hostname 分别为 ws6504D 和 Z2FN1。其中 ws6504D 为核心交换机，由于思科网络助手无法管理三层交换机，所以将其列入 Neighbors 组，而 Z2FN1 根据命名可知其是属于网络 A 中的交换机，不属于网络 B，而网络 A、B 应为物理隔离，不应有关联，所以可判断 Z2FN1 这台交换机与网络 B 中的某一台交换机发生了不应有的连接。

观察右侧区域拓扑，与 Z2FN1 相连的交换机为 Z2FD1（放大后如图 3 所示），Z2FN1 和 Z2FD1 均位于综合楼二楼配线间。在综合楼二楼配线间，现场勘查 Z2FD1 和 Z2FN1 这两台交换机之间并未发生互连，则互连必发生在工作区。查看网络端口表可知，与 Z2FN1 的 Fa0/46 端口和 Z2FD1 的 Fa0/40 端口相连的信息插座均位于综合楼一楼的同一间办公室。经在该办公室现场勘查，发现用户私接了一台 8 口的微型交换机，该交换机用两条网线同时连接了信息插座中分属网络 A、B 的两个网口。将其中一条网线拔掉，在思科网络助手中刷新拓扑图，发现交换机 Z2FN1 消失了，说明网络 A、B 间的连接已被清除。

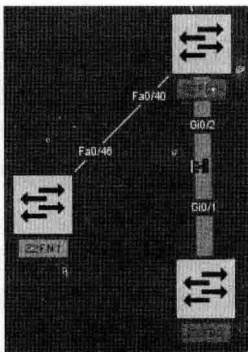


图 3 发生错误互连的两台交换机

其实用命令行的方式也能发现和排除此类故障。

首先逐一 telnet 网络 B 中的每台交换机，用 show cdp neighbors 命令查看其相邻的交换机是哪几个，根据 hostname 名判断其是否属于本网络，如果发现相邻交换机不属于本网络，则可判定已找到发生错误连接的两台交换机（如图 4 所示）。此方法需遍历 community 中的所有交换机，需反复输入 telnet 登录口令并重复手工敲入命令，效率低下，远不及使用 CAN 方便和高效。

```

C22F02>show cdp neighbors
Capability Codes: R - Router, T - Trans Bridge, B - Source Route Bridge
                  S - Switch, H - Host, I - IGMP, F - Filter, P - Phone

Device ID      Local Interface   Remote      Remote      Capability Platform Port ID
-----
C22F02        G1g 0/21          159        R S I      UC-C2948- G1g 2/1
C22F02        Fa 0/18           179        S I        UC-C2948- Fa 0/40
C22F02        G1g 0/2           135        S I        UC-C2948- G1g 0/1
    
```

图 4 用 show cdp neighbors 命令查看其相邻的交换机

系统升级惹麻烦

浙江 陈智好

故障现象

一天早上，接到终端用户的电话：“我的笔记本电脑系统无法登录了，画面内容提示的是配置 Windows Update 失败，还原更改，请勿关机。但我已经等了一个多小时，还原失败了，无法登录啊。”拿到这台有问题的笔记本电脑，打开一看，屏幕画面一直停留在用户所说的提示状态。

故障排查

解决无法正常登录系统的办法，一般思路是看能否进入“安全模式”，如果能进“安全模式”，就可以尝试解决此问题。

首先关机，重新启动系统，按 F8 键选择“安全模式”进入 Windows 7 系统，稍等片刻，系统可以正常进入“安全模式”。根据上述屏幕登录画面的提示，Windows 7 系统应该是系统升级过程中出错导致，只要顺着这条线索，找到“控制面板”中的“系统和安全”选项，选择“Windows Update”中的“更改设置”菜单，选择“重要更新”更改为“从不检查更新”，并且去除勾选“允许所有用户在此计算机上安装更新”选项，应该就能解决问题了。但是，

当查看“控制面板”时，发现在“安全模式”下无法找到“Windows Update”。

图 1 是正常启动系统与安全模式启动后系统内“系统和安全”选项对比图。



图 1 正常启动系统与安全模式启动后系统内“系统和安全”选项对比

到此，通过关闭 Windows Update 修复无法登录问题无法解决。

故障排除

关闭 Windows Update 和去除勾选“允许所有用户在此计算机上安装更新”选项的操作，让笔者想到可能是更新的安装文件无法正常安装完成导致，如果卸载了这些更新，是否能解决登录问题呢？

马上找到“控制面板”中“程序”选项，选择“程序和功能”中“查看已安装的更新”一项（如图 2 所示），确定系统最近更新过三个更新包。依次卸载这三个

Windows 更新后，重启系统，即可正常登录 Windows 系统了。

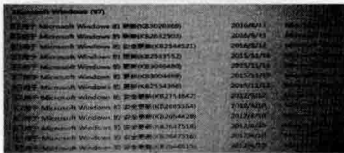


图 2 查看已安装的更新

经验总结

通过这次问题的解决，笔者发现在系统问题故障出现的情况下，可以从系统给出的提示或者反馈信息中找到解决故障的线索，依据这些线索思考解决问题的办法，尝试不同的操作。这样的操作比起遇到系统问题，即利用重装系统来解决，更能锻炼解决问题的能力。

路由器兼容性故障案例

福建 林雄

在单位网络机房建设中，更换了很多网络交换设备，不可避免地碰到很多路由器兼容性故障，特别是不同品牌路由器的兼容性问题，其中以华为路由器与思科路由器的兼容为主，具体以案例形式描述如下。

案例一：路由器协议不匹配

网络结构如图 1 所示，故障原因是，思科路由器和华为路由器的默认协议不同，前者为 HDLC，后者为 PPP，在路由器的配置中，很容易发现这个问题，也很好解决，在路由器的端口封装协议时，双方一致就可以了。

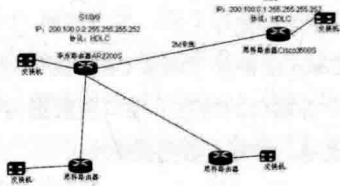


图 1 案例一设备网络连接图

案例二：路由器时钟匹配问题

1. 故障现象

在更换路由器设备时，将原来思科路由器的网络参数，配置到华为路由器上后，以为这样应该问题不大，但在应用中出现了路由器端口状态异常，具体现象为，

链路协议有时 Up 有时 Down 或直接 Down。

当时 Cisco 3600S 和 AR2200S 两端接口配置分别是：

Cisco 设备 Serial 口配置如下：

```
interface Serial0/0
enc hdlc
ip address 200.100.0.1 255.255.255.252
```

AR2200S 的 Serial 口配置如下：

```
interface Serial1/0/0
link-protocol hdlc
ip address 200.100.0.2 255.255.255.252
```

2. 故障分析

网络参数配置没有问题，两端均配置 HDLC 协议，两端 Serial 端口均启用（网络链路状态为 Up，协议为 Down），那出现的情况可能就是两个不同设备间 HDLC 协议的差异。

经查询发现，国内某个项目在使用华为路由器替换 Cisco 路由器时也出现这样的问题：使用 Serial 口对接 Cisco 设置对接互联时，端口起不来，一直处于 Down 的状态。

故障原因是线路上的时钟错位，导致线路两端路由器收和发不能同步引起，在接口上将时钟反转 invert receive-clock 后相当于使时钟改变半个周期而使时钟对准。

3. 故障解决

在华为路由器的 Serial 口下配置如下命令：

invert receive-clock auto

之后, 路由器端口状态恢复正常。

invert receive-clock 命令用来允许反转 DTE 侧同步串口的接收时钟信号。undo invert receive-clock 命令用来恢复缺省情况。缺省情况下, 同步串口作为 DTE 侧时, 禁止翻转接收时钟信号。

注意

DTE 与 DCE 的区别, 其区分只是针对串行端口的, 路由器通过串行端口连接广域网络。用于接口的区分, 比如一台路由器, 它处于网络的边缘, 它有一个 S0 口需要从另一台路由器中学习到一些参数, 具体实施时, 我们就不需在这个 S0 口配“时钟速率”, 它从对方学到。这时它就是 DTE, 而对方就是 DCE。

案例三：路由器带宽匹配问题

1. 故障现象

网络传输数据时网络延迟很大, 达到上千毫秒, 或是直接 time out, 查询 Serial 端口信息发现带宽占用率达百分之百, 如图 2 所示。

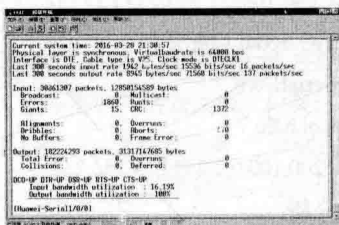


图 2 接口输出带宽占用率

2. 故障分析

首先用开其他网络设备, 测试两端路由器联通情况, 发现网络十分稳定, 接入单个用户时延迟并不明显。再次接入几个正常业务, 网络延迟大增, display interface 端口信息发现数据量不大, 误码率也很小, 如图 3 所示。

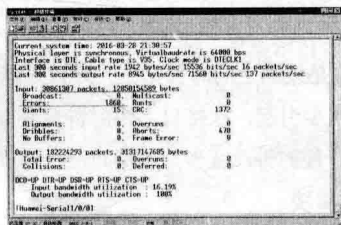


图 3 接口输出信息量

使用抓包工具进行抓包并没有发现不正常的数据通信。

经过仔细查看信息后发现 Serial 端口下速率竟为 64K (如图 4 所示)。

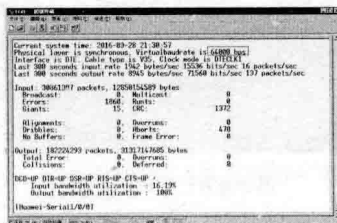


图 4 接口速率

Physical layer is synchronous, Virtualbaudrate is 64000 bps

而传输设备数据为 2048K, 思科设备默认 Serial 端口速率为 2048K, 而华为 AR2200S 路由器的默认设置为 64K, 造成网络带宽限制为只有 64K, 原来在 2M 线下的业务当然会造成在 64K 的线路不稳定了。

3. 故障解决

此时 Cisco 3600S 和 AR2200S 两端接口正确的配置分别是:

Cisco 设备 Serial 口配置如下:

```
interface Serial0/0
enc hdslc
ip address 200.100.0.1 255.255.255.252
```

AR2204 的 Serial 口配置如下:

```
interface Serial1/0/0
link-protocol hdslc
ip address 200.100.0.2 255.255.255.252
virtualbaudrate 2048000
invert receive-clock auto
```

由此得出以下结论:

在替换 Cisco 设备并与原来 Cisco 设备对接时, 首先要认真查看设备端口的信息, 端口间数据传输无外乎协议、IP 地址规划、带宽、数据误码率。

分析方法

在路由器中分析内部网络问题, 在不影响现有网络状态的情况下, 最直接有效的方法就是进行抓包, 针对这方面的问题, 我们可以路由器端口镜像功能实现在 PC 上抓包分析, 这样即不影响路由操作, 可以逐个端口并且分输入、输出端进行排查分析, 也能根据详细的数据包信息直观地发现网络问题。

以华为 AR2200S 路由器为例:

使用 `dis int brief` 命令查询接口的汇总信息如图 5 所示。

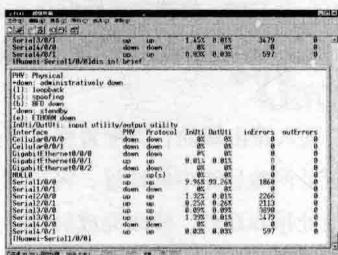


图 5 接口的汇总信息

此时发现端口 Serial1/0/0 输入端带宽占用率达 93.26%。接下来我们分析 Serial1/0/0 端口数据包。

首先将 Serial1/0/0 端口镜像到以太网口 GigabitEthernet 0/0/2 网口以便进行抓包。

在系统配置模式下：

[Huawei]observe-port interface GigabitEthernet 0/0/2

设置以太网口 3 为镜像口

在端口 Serial1/0/0 配置模式下：

[Huawei-Serial1/0/0]mirror to observe-port outbound

将输出端镜像至以太网口 3

[Huawei-Serial1/0/0]mirror to observe-port inbound

将输入端镜像至以太网口 3

将 PC 接入以太网 3，不需要配置 IP 地址，使用抓包软件进行抓包，我们以 IpTool 工具为例（如图 6 所示），可以看到，PC 机以太网口接收到大量广播包，此时便可以根据相关数据进行分析排查问题。

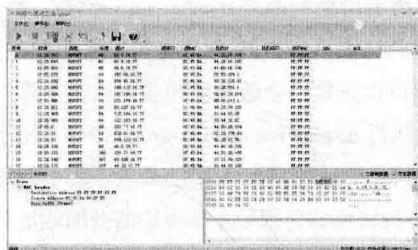


图 6 网络抓包信息

NAT 配置不当网异常

故障现象

单位因 IP 地址不足，在 1 台华为 AR2200 路由器上启用了 NAT 地址转换，提高路由器工作效率和减少路由器工作负荷。管理员给 NAT 地址池分配了两个连续的 C 类地址供用户使用，确保大部分用户可以通过 NAT 地址转换的方式访问公网。

在完成 NAT 配置并进行测试过程中，先后出现了以下三个故障现象：一是在配置完成并进行测试时，刚开始各用户上网均正常，但在上网高峰期，有用户反馈访问公网网站无法访问，但是能 Ping 通访问公网网站的 IP 地址。二是在重新配置后，所有用户均可以正常上网。但是过了一段时间后，个别用户突然出现不能上网的现象，需要重新获取 IP 地址或手动修改 IP 地址后才能正常访问公网。三是因用户过多，对原有两个 C 类地址池进行了扩展，将原有两个 C 类地址扩展为一个 B 类地址，

配置修改完成后，发现路由器不能进行正常的 NAT 转换，修改回原来的配置后，故障也没有排除。

故障分析

故障一：在路由器上执行 `display nat statistics` 命令（用于查看 NAT 相关信息和统计信息的命令），通过查看 NAT 的统计信息，发现出现路由器接收到大量 NAT 请求报文，但很多都转发失败，而且失败的报文数量增长非常快。继续执行命令 `display nat session`（用于查看 NAT 连接会话请求和建立状态的命令），发现没有异常的会话建立。继续执行命令 `display nat users`（用于查看 NAT 用户连接数目的命令），发现用户的连接数超出允许的最大连接数，原来华为路由器默认的最大连接数为 500，当用户的连接数超出最大连接数时，会话就无法建立。

福建泉州 王刚 叶永安 陈柳君

故障二：有计算机可以正常上网，说明 NAT 地址转换没有问题，在不能上网的用户计算机上查看其计算机 IP 地址，发现其 IP 地址可以正常获取，IP 地址也在地址池内，但就是无法访问公网，Ping 公网网站 IP 地址，也无法 Ping 通。但在路由器内分别 Ping 公网网站 IP 地址和该用户计算机 IP 地址，却均可以 Ping 通。手动修改该计算机为其他 IP 地址，发现可以上网，看来应该是 NAT 地址转换配置存在问题。

在路由器中执行命令 `display nat session`，检查发现，不能上网的计算机用户 IP 地址有转换表项和建立会话，相应的端口也正常，会话请求和建立状态正常。继续在路由器上执行 `display nat address-group` 命令（用于查看地址池中内网公网地址转换结果），发现不能上网用户计算机 IP 地址被转换成公网后是不可用的公网地址，被转换后的公网地址是地址池中掩码相与后的网络广播地址。原来在配置 NAT 地址池时，将公网网络的网络地址和广播地址都包括到里面去了，在 NAT 地址转换后，转换成了不能使用的广播地址。

故障三：在将地址池进行扩展后，发现内网用户均不能上网，Ping 公网网站也无法 Ping 通，而从公网使用 `tracert` 地址池 IP 地址，发现正常，看来是 NAT 配置存在问题。在路由器中执行命令 `display ip routing-table`（用于查看路由条目的命令），查看地址池对应的黑洞路由是否正确配置，命令显示没有新增地址对应的黑洞路由条目。在路由器启用 NAT 地址转换后，为避免环路，一般都会配置黑洞路由，配置黑洞一般均采用静态手动配置，也可以自动生成，配置黑洞路由一般使用 `null 0` 接口，因该接口永远不会 Down，管理员手动将某个地址转换到 `null 0` 接口，这样对系统负载影响非常小。当然也可以使用 ACL 方法实现该功能，但会增加路由器的 CPU 占用率，一般不采用这种方法。

故障排除

找到了故障原因，故障就好排除了。

故障一：进入路由器的管理配置模式并进入系统视

图，执行命令 `nat service-class class connections 1200`，修改默认连接数 500 为 1200，修改完成后保存并重启路由器，再执行 `display nat users`，发现在线用户没有超过 1200 这个数量，故障排除。

故障二：进入路由器的管理配置模式并进入系统视图，重新设置公网地址池中的地址，将公网地址的网络地址和广播地址排除在外，修改完成后保存并重启路由器，故障排除。

故障三：进入路由器的管理配置模式并进入系统视图，执行命令 `ip route-static X.X.X.X 32 null 0`（X.X.X.X 为公网 IP 地址）手动增加黑洞静态路由。配置完成后，系统会自动给 NAT 地址池中的每一个地址生成一条指向 `null 0` 的 32 位掩码的路由，就实现了 NAT 反向转换，修改完成后保存并重启路由器，故障排除。

经验总结

当内网用户较多，并且出现网页打开慢甚至出现网页打不开的现象时，应该首先检查 NAT 转换是否成功，可以使用相关命令查看用户连接数目是否超过限定的数目（如图 1 所示），如果超出就需要修改 NAT 的最大连接数。在配置 NAT 地址转换功能时，需要注意地址池中的地址不能包含和地址池公网网络的广播地址和网络地址。在对 NAT 地址池扩展后，需要增加新的黑洞静态路由，否则 NAT 功能将不能使用。

```

<Huawei> display nat session all verbose
NAT Session Table Information:

Protocol      : TCP(6)
SrcAddr Port Vpn : 10.200.200.200 65532
DestAddr Port Vpn : 10.100.100.100 1024
Time To Live   : 60 s
NAT-Info
  New SrcAddr   : 10.10.10.10
  New SrcPort   : 10240
  New DestAddr  : 10.30.30.30
  New DestPort  : 21

Protocol      : UDP(6)
SrcAddr Port Vpn : 10.200.200.200 65532
DestAddr Port Vpn : 10.100.100.100 1024
Time To Live   : 60 s
NAT-Info
  New SrcAddr   : 10.10.10.10
  New SrcPort   : 10240
  New DestAddr  : 10.30.30.3
  New DestPort  : 21
    
```

图 1 NAT 连接用户详情

地址重复引发路由故障

山东 何钰 崔冬梅

故障现象

近日，有同事反映某服务器不能正常访问，得知这一故障现象后，我们进行了故障现象的还原，最后得知位于 YZ-BRAS 下的一台服务器不能正常访问，而位于其他地区的服务器访问正常。出现故障的服务器和能正常访问的服务器位于不同的 BRAS 上。

故障分析

首先我们了解下网络拓扑结构，JN-BRAS 和 YZ-BRAS 两台 BRAS 上联两台核心路由器形成双归属结构。然后服务器位于 YZ-BRAS 下的汇聚交换机上（如图 1 所示）。

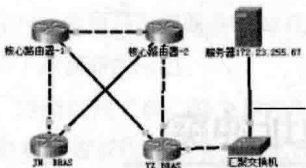


图 1 网络拓扑结构

通过图 1 我们可以看到，位于 JN-BRAS 下的用户欲访问 YZ-BRAS 下的服务器 172.23.255.67，结果是不能成功的。其实网络结构十分简单。紧接着得知位于 JN-BRAS 下的宽带拨号用户获取到的 IP 地址是 10.219.80.5，在该 PC 机上是不能正常 Ping 通 172.23.255.67 这台服务器，trace 的结果是只能到达核心路由器-1，而在核心路由器-1 上是可以 Ping 通 172.23.255.67 这台服务器。所以可以初步断定在核心路由器上路由出现问题。但在核心路由器-1 上使用命令 show ip forwarding route 172.23.255.67，可以学习到 172.23.255.67 的路由。

问题分析到这里，似乎感觉是路由学习出现了问题，但是在两台核心路由器上反复使用命令 show ip bgp neighbor in 10.253.138.3 查看学习到 YZ-BRAS 路由情况，如图 2 所示。

```
SDG-JN-CR-T3000-1#show ip bgp neighbor in 10.253.138.3
Routes Learned From This Neighbor:
Status codes: * valid, > best, i - internal, s - stale
Origin codes: i - IGP, e - EGP, ? - incomplete
Network          Next Hop        Metric      LocPrf      RtrPrf  Path
*10.181.0.0/16    10.253.0.5       100          200         ?       i
*10.178.0.0/16    10.253.0.5       100          200         ?       i
*10.182.0.0/16    10.253.0.5       100          200         ?       i
*10.227.0.0/16    10.253.0.27      100          200         ?       i
*10.143.0.0/16    10.253.0.27      100          200         ?       i
*10.142.0.0/16    10.253.0.27      100          200         ?       i
SDG-JN-CR-T3000-1#show ip bgp neighbor in 10.253.138.3
Routes Learned From This Neighbor:
Status codes: * valid, > best, i - internal, s - stale
Origin codes: i - IGP, e - EGP, ? - incomplete
Network          Next Hop        Metric      LocPrf      RtrPrf  Path
*10.103.244.254/29 10.253.138.3     100          200         ?       ?
*10.172.23.254/27 10.253.138.3     100          200         ?       ?
*10.219.184.0/21 10.253.138.3     100          200         ?       ?
*10.219.200.0/23 10.253.138.3     100          200         ?       ?
*10.253.140.0/30 10.253.138.3     100          200         ?       ?
*10.253.139.0/30 10.253.138.3     100          200         ?       ?
*10.108.138.0/17 10.253.138.3     100          200         ?       ?
*10.219.12.64/26 10.253.138.3     100          200         ?       ?
*10.219.33.0/24 10.253.138.3     100          200         ?       ?
*10.219.34.0/24 10.253.138.3     100          200         ?       ?
*10.219.36.0/24 10.253.138.3     100          200         ?       ?
*10.219.44.0/23 10.253.138.3     100          200         ?       ?
*10.219.46.0/23 10.253.138.3     100          200         ?       ?
*10.253.138.0/32 10.253.138.3     100          200         ?       ?
*10.172.23.254/27 10.253.138.3     100          200         ?       ?
*10.172.25.0/24 10.253.138.3     100          200         ?       ?
*10.172.27.0/24 10.253.138.3     100          200         ?       ?
SDG-JN-CR-T3000-1#show ip bgp neighbor in 10.253.138.1 济宁BRAS
Routes Learned From This Neighbor:
Status codes: * valid, > best, i - internal, s - stale
Origin codes: i - IGP, e - EGP, ? - incomplete
Network          Next Hop        Metric      LocPrf      RtrPrf  Path
*10.220.255.16/29 10.253.138.1     100          200         ?       ?
*10.254.138.0/20 10.253.138.1     100          200         ?       ?
*10.200.0.0/24 10.253.138.1     100          200         ?       ?
*172.0.0.0/8 10.253.138.1     100          200         ?       ?
*10.222.253.0/24 10.253.138.1     100          200         ?       ?
*10.220.207.0/24 10.253.138.1     100          200         ?       ?
*172.28.0.0/9 10.253.138.1     100          200         ?       ?
*10.220.255.0/29 10.253.138.1     100          200         ?       ?
*10.255.0.0/17 10.253.138.1     100          200         ?       ?
*10.66.44.0/21 10.253.138.1     100          200         ?       ?
*10.107.0.0/16 10.253.138.1     100          200         ?       ?
*10.219.4.0/22 10.253.138.1     100          200         ?       ?
*10.219.8.0/22 10.253.138.1     100          200         ?       ?
*10.219.12.0/22 10.253.138.1     100          200         ?       ?
*10.219.16.0/22 10.253.138.1     100          200         ?       ?
*10.219.20.0/22 10.253.138.1     100          200         ?       ?
*10.219.24.0/22 10.253.138.1     100          200         ?       ?
*10.219.28.0/22 10.253.138.1     100          200         ?       ?
*10.220.224.0/20 10.253.138.1     100          200         ?       ?
*10.254.138.0/20 10.253.138.1     100          200         ?       ?
*10.191.144.0/20 10.253.138.1     100          200         ?       ?
*10.220.240.0/21 10.253.138.1     100          200         ?       ?
*10.220.254.0/23 10.253.138.1     100          200         ?       ?
*10.253.138.1/32 10.253.138.1     100          200         ?       ?
*172.24.0.0/17 10.253.138.1     100          200         ?       ?
*10.253.140.0/30 10.253.138.1     100          200         ?       ?
*10.253.139.0/30 10.253.138.1     100          200         ?       ?
*10.219.52.0/22 10.253.138.1     100          200         ?       ?
*10.219.80.0/20 10.253.138.1     100          200         ?       ?
*10.219.144.0/24 10.253.138.1     100          200         ?       ?
SDG-JN-CR-T3000-1# show run
```

图 2 在核心路由器-1 上学习 YZ-BRAS 的路由情况示意图

通过图 2 可以看到，172.23.154.64/27 网段已经从 YZ-BRAS 学习到，那么在核心路由器-1 上能否学习到来自 JN-BRAS10.219.80.0 网段的路由呢？使用命令 show ip bgp neighbor in 10.253.138.1 查看，如图 3 所示。

```
SDG-JN-CR-T3000-1#show ip bgp neighbor in 10.253.138.1 济宁BRAS
Routes Learned From This Neighbor:
Status codes: * valid, > best, i - internal, s - stale
Origin codes: i - IGP, e - EGP, ? - incomplete
Network          Next Hop        Metric      LocPrf      RtrPrf  Path
*10.220.255.16/29 10.253.138.1     100          200         ?       ?
*10.254.138.0/20 10.253.138.1     100          200         ?       ?
*10.200.0.0/24 10.253.138.1     100          200         ?       ?
*172.0.0.0/8 10.253.138.1     100          200         ?       ?
*10.222.253.0/24 10.253.138.1     100          200         ?       ?
*10.220.207.0/24 10.253.138.1     100          200         ?       ?
*172.28.0.0/9 10.253.138.1     100          200         ?       ?
*10.220.255.0/29 10.253.138.1     100          200         ?       ?
*10.255.0.0/17 10.253.138.1     100          200         ?       ?
*10.66.44.0/21 10.253.138.1     100          200         ?       ?
*10.107.0.0/16 10.253.138.1     100          200         ?       ?
*10.219.4.0/22 10.253.138.1     100          200         ?       ?
*10.219.8.0/22 10.253.138.1     100          200         ?       ?
*10.219.12.0/22 10.253.138.1     100          200         ?       ?
*10.219.16.0/22 10.253.138.1     100          200         ?       ?
*10.219.20.0/22 10.253.138.1     100          200         ?       ?
*10.219.24.0/22 10.253.138.1     100          200         ?       ?
*10.219.28.0/22 10.253.138.1     100          200         ?       ?
*10.220.224.0/20 10.253.138.1     100          200         ?       ?
*10.254.138.0/20 10.253.138.1     100          200         ?       ?
*10.191.144.0/20 10.253.138.1     100          200         ?       ?
*10.220.240.0/21 10.253.138.1     100          200         ?       ?
*10.220.254.0/23 10.253.138.1     100          200         ?       ?
*10.253.138.1/32 10.253.138.1     100          200         ?       ?
*172.24.0.0/17 10.253.138.1     100          200         ?       ?
*10.253.140.0/30 10.253.138.1     100          200         ?       ?
*10.253.139.0/30 10.253.138.1     100          200         ?       ?
*10.219.52.0/22 10.253.138.1     100          200         ?       ?
*10.219.80.0/20 10.253.138.1     100          200         ?       ?
*10.219.144.0/24 10.253.138.1     100          200         ?       ?
SDG-JN-CR-T3000-1# show run
```

图 3 核心路由器学习 JN-BRAS 路由情况示意图

通过图 3 可以看到，核心路由器也能学习到来自 10.219.80.0/20 的路由，这样就可以断定核心路由器分别从两台 BRAS 学习到了两个网段的路由。但是为什么两者不能通讯呢？

故障排除

接下来在 YZ-BRAS 进行路由查看，具体的命令

是 show ip bgp neighbor in 10.253.0.19, 在这里我们可以清楚地看到 YZ-BRAS 学习到的路由都是汇总路由即 10.219.0.0/16 等。这是因为在核心路由器的 BGP 路由中已经将网段进行了汇总, 具体命令是 aggregate-address 10.219.0.0 255.255.0.0 count 0 summary-only, 意思也就是说核心路由器只向外发布聚合后的路由, 这就是为什么 YZ-BRAS 只能学习到汇总路由的缘故。在 YZ-BRAS 上查看 10.219.80.0/20 的路由转发表时, 可以看到问题的端倪 (如图 4 所示)。

```

show ip forwarding route 10.219.80.0
IPV4 Routing Table
Header: Src: Destination, Gw: Gateway, Pri: Priority
Codes: S: Static, B: BGP, I: IGMP, O: OSPF, D: DDP, E: EIGRP, H: HSRP, L: LSP, N: NHRP, P: PIM, R: RIP, T: TFTP, U: User-defined, V: VRRP, W: WCCP, X: X.25, Y: Y.28, Z: Z.39, A: A.1, B: B.2, C: C.3, D: D.4, E: E.5, F: F.6, G: G.7, H: H.8, I: I.9, J: J.10, K: K.11, L: L.12, M: M.13, N: N.14, O: O.15, P: P.16, Q: Q.17, R: R.18, S: S.19, T: T.20, U: U.21, V: V.22, W: W.23, X: X.24, Y: Y.25, Z: Z.26, A: A.27, B: B.28, C: C.29, D: D.30, E: E.31, F: F.32, G: G.33, H: H.34, I: I.35, J: J.36, K: K.37, L: L.38, M: M.39, N: N.40, O: O.41, P: P.42, Q: Q.43, R: R.44, S: S.45, T: T.46, U: U.47, V: V.48, W: W.49, X: X.50, Y: Y.51, Z: Z.52, A: A.53, B: B.54, C: C.55, D: D.56, E: E.57, F: F.58, G: G.59, H: H.60, I: I.61, J: J.62, K: K.63, L: L.64, M: M.65, N: N.66, O: O.67, P: P.68, Q: Q.69, R: R.70, S: S.71, T: T.72, U: U.73, V: V.74, W: W.75, X: X.76, Y: Y.77, Z: Z.78, A: A.79, B: B.80, C: C.81, D: D.82, E: E.83, F: F.84, G: G.85, H: H.86, I: I.87, J: J.88, K: K.89, L: L.90, M: M.91, N: N.92, O: O.93, P: P.94, Q: Q.95, R: R.96, S: S.97, T: T.98, U: U.99, V: V.100, W: W.101, X: X.102, Y: Y.103, Z: Z.104, A: A.105, B: B.106, C: C.107, D: D.108, E: E.109, F: F.110, G: G.111, H: H.112, I: I.113, J: J.114, K: K.115, L: L.116, M: M.117, N: N.118, O: O.119, P: P.120, Q: Q.121, R: R.122, S: S.123, T: T.124, U: U.125, V: V.126, W: W.127, X: X.128, Y: Y.129, Z: Z.130, A: A.131, B: B.132, C: C.133, D: D.134, E: E.135, F: F.136, G: G.137, H: H.138, I: I.139, J: J.140, K: K.141, L: L.142, M: M.143, N: N.144, O: O.145, P: P.146, Q: Q.147, R: R.148, S: S.149, T: T.150, U: U.151, V: V.152, W: W.153, X: X.154, Y: Y.155, Z: Z.156, A: A.157, B: B.158, C: C.159, D: D.160, E: E.161, F: F.162, G: G.163, H: H.164, I: I.165, J: J.166, K: K.167, L: L.168, M: M.169, N: N.170, O: O.171, P: P.172, Q: Q.173, R: R.174, S: S.175, T: T.176, U: U.177, V: V.178, W: W.179, X: X.180, Y: Y.181, Z: Z.182, A: A.183, B: B.184, C: C.185, D: D.186, E: E.187, F: F.188, G: G.189, H: H.190, I: I.191, J: J.192, K: K.193, L: L.194, M: M.195, N: N.196, O: O.197, P: P.198, Q: Q.199, R: R.200, S: S.201, T: T.202, U: U.203, V: V.204, W: W.205, X: X.206, Y: Y.207, Z: Z.208, A: A.209, B: B.210, C: C.211, D: D.212, E: E.213, F: F.214, G: G.215, H: H.216, I: I.217, J: J.218, K: K.219, L: L.220, M: M.221, N: N.222, O: O.223, P: P.224, Q: Q.225, R: R.226, S: S.227, T: T.228, U: U.229, V: V.230, W: W.231, X: X.232, Y: Y.233, Z: Z.234, A: A.235, B: B.236, C: C.237, D: D.238, E: E.239, F: F.240, G: G.241, H: H.242, I: I.243, J: J.244, K: K.245, L: L.246, M: M.247, N: N.248, O: O.249, P: P.250, Q: Q.251, R: R.252, S: S.253, T: T.254, U: U.255, V: V.256, W: W.257, X: X.258, Y: Y.259, Z: Z.260, A: A.261, B: B.262, C: C.263, D: D.264, E: E.265, F: F.266, G: G.267, H: H.268, I: I.269, J: J.270, K: K.271, L: L.272, M: M.273, N: N.274, O: O.275, P: P.276, Q: Q.277, R: R.278, S: S.279, T: T.280, U: U.281, V: V.282, W: W.283, X: X.284, Y: Y.285, Z: Z.286, A: A.287, B: B.288, C: C.289, D: D.290, E: E.291, F: F.292, G: G.293, H: H.294, I: I.295, J: J.296, K: K.297, L: L.298, M: M.299, N: N.300, O: O.301, P: P.302, Q: Q.303, R: R.304, S: S.305, T: T.306, U: U.307, V: V.308, W: W.309, X: X.310, Y: Y.311, Z: Z.312, A: A.313, B: B.314, C: C.315, D: D.316, E: E.317, F: F.318, G: G.319, H: H.320, I: I.321, J: J.322, K: K.323, L: L.324, M: M.325, N: N.326, O: O.327, P: P.328, Q: Q.329, R: R.330, S: S.331, T: T.332, U: U.333, V: V.334, W: W.335, X: X.336, Y: Y.337, Z: Z.338, A: A.339, B: B.340, C: C.341, D: D.342, E: E.343, F: F.344, G: G.345, H: H.346, I: I.347, J: J.348, K: K.349, L: L.350, M: M.351, N: N.352, O: O.353, P: P.354, Q: Q.355, R: R.356, S: S.357, T: T.358, U: U.359, V: V.360, W: W.361, X: X.362, Y: Y.363, Z: Z.364, A: A.365, B: B.366, C: C.367, D: D.368, E: E.369, F: F.370, G: G.371, H: H.372, I: I.373, J: J.374, K: K.375, L: L.376, M: M.377, N: N.378, O: O.379, P: P.380, Q: Q.381, R: R.382, S: S.383, T: T.384, U: U.385, V: V.386, W: W.387, X: X.388, Y: Y.389, Z: Z.390, A: A.391, B: B.392, C: C.393, D: D.394, E: E.395, F: F.396, G: G.397, H: H.398, I: I.399, J: J.400, K: K.401, L: L.402, M: M.403, N: N.404, O: O.405, P: P.406, Q: Q.407, R: R.408, S: S.409, T: T.410, U: U.411, V: V.412, W: W.413, X: X.414, Y: Y.415, Z: Z.416, A: A.417, B: B.418, C: C.419, D: D.420, E: E.421, F: F.422, G: G.423, H: H.424, I: I.425, J: J.426, K: K.427, L: L.428, M: M.429, N: N.430, O: O.431, P: P.432, Q: Q.433, R: R.434, S: S.435, T: T.436, U: U.437, V: V.438, W: W.439, X: X.440, Y: Y.441, Z: Z.442, A: A.443, B: B.444, C: C.445, D: D.446, E: E.447, F: F.448, G: G.449, H: H.450, I: I.451, J: J.452, K: K.453, L: L.454, M: M.455, N: N.456, O: O.457, P: P.458, Q: Q.459, R: R.460, S: S.461, T: T.462, U: U.463, V: V.464, W: W.465, X: X.466, Y: Y.467, Z: Z.468, A: A.469, B: B.470, C: C.471, D: D.472, E: E.473, F: F.474, G: G.475, H: H.476, I: I.477, J: J.478, K: K.479, L: L.480, M: M.481, N: N.482, O: O.483, P: P.484, Q: Q.485, R: R.486, S: S.487, T: T.488, U: U.489, V: V.490, W: W.491, X: X.492, Y: Y.493, Z: Z.494, A: A.495, B: B.496, C: C.497, D: D.498, E: E.499, F: F.500, G: G.501, H: H.502, I: I.503, J: J.504, K: K.505, L: L.506, M: M.507, N: N.508, O: O.509, P: P.510, Q: Q.511, R: R.512, S: S.513, T: T.514, U: U.515, V: V.516, W: W.517, X: X.518, Y: Y.519, Z: Z.520, A: A.521, B: B.522, C: C.523, D: D.524, E: E.525, F: F.526, G: G.527, H: H.528, I: I.529, J: J.530, K: K.531, L: L.532, M: M.533, N: N.534, O: O.535, P: P.536, Q: Q.537, R: R.538, S: S.539, T: T.540, U: U.541, V: V.542, W: W.543, X: X.544, Y: Y.545, Z: Z.546, A: A.547, B: B.548, C: C.549, D: D.550, E: E.551, F: F.552, G: G.553, H: H.554, I: I.555, J: J.556, K: K.557, L: L.558, M: M.559, N: N.560, O: O.561, P: P.562, Q: Q.563, R: R.564, S: S.565, T: T.566, U: U.567, V: V.568, W: W.569, X: X.570, Y: Y.571, Z: Z.572, A: A.573, B: B.574, C: C.575, D: D.576, E: E.577, F: F.578, G: G.579, H: H.580, I: I.581, J: J.582, K: K.583, L: L.584, M: M.585, N: N.586, O: O.587, P: P.588, Q: Q.589, R: R.590, S: S.591, T: T.592, U: U.593, V: V.594, W: W.595, X: X.596, Y: Y.597, Z: Z.598, A: A.599, B: B.600, C: C.601, D: D.602, E: E.603, F: F.604, G: G.605, H: H.606, I: I.607, J: J.608, K: K.609, L: L.610, M: M.611, N: N.612, O: O.613, P: P.614, Q: Q.615, R: R.616, S: S.617, T: T.618, U: U.619, V: V.620, W: W.621, X: X.622, Y: Y.623, Z: Z.624, A: A.625, B: B.626, C: C.627, D: D.628, E: E.629, F: F.630, G: G.631, H: H.632, I: I.633, J: J.634, K: K.635, L: L.636, M: M.637, N: N.638, O: O.639, P: P.640, Q: Q.641, R: R.642, S: S.643, T: T.644, U: U.645, V: V.646, W: W.647, X: X.648, Y: Y.649, Z: Z.650, A: A.651, B: B.652, C: C.653, D: D.654, E: E.655, F: F.656, G: G.657, H: H.658, I: I.659, J: J.660, K: K.661, L: L.662, M: M.663, N: N.664, O: O.665, P: P.666, Q: Q.667, R: R.668, S: S.669, T: T.670, U: U.671, V: V.672, W: W.673, X: X.674, Y: Y.675, Z: Z.676, A: A.677, B: B.678, C: C.679, D: D.680, E: E.681, F: F.682, G: G.683, H: H.684, I: I.685, J: J.686, K: K.687, L: L.688, M: M.689, N: N.690, O: O.691, P: P.692, Q: Q.693, R: R.694, S: S.695, T: T.696, U: U.697, V: V.698, W: W.699, X: X.700, Y: Y.701, Z: Z.702, A: A.703, B: B.704, C: C.705, D: D.706, E: E.707, F: F.708, G: G.709, H: H.710, I: I.711, J: J.712, K: K.713, L: L.714, M: M.715, N: N.716, O: O.717, P: P.718, Q: Q.719, R: R.720, S: S.721, T: T.722, U: U.723, V: V.724, W: W.725, X: X.726, Y: Y.727, Z: Z.728, A: A.729, B: B.730, C: C.731, D: D.732, E: E.733, F: F.734, G: G.735, H: H.736, I: I.737, J: J.738, K: K.739, L: L.740, M: M.741, N: N.742, O: O.743, P: P.744, Q: Q.745, R: R.746, S: S.747, T: T.748, U: U.749, V: V.750, W: W.751, X: X.752, Y: Y.753, Z: Z.754, A: A.755, B: B.756, C: C.757, D: D.758, E: E.759, F: F.760, G: G.761, H: H.762, I: I.763, J: J.764, K: K.765, L: L.766, M: M.767, N: N.768, O: O.769, P: P.770, Q: Q.771, R: R.772, S: S.773, T: T.774, U: U.775, V: V.776, W: W.777, X: X.778, Y: Y.779, Z: Z.780, A: A.781, B: B.782, C: C.783, D: D.784, E: E.785, F: F.786, G: G.787, H: H.788, I: I.789, J: J.790, K: K.791, L: L.792, M: M.793, N: N.794, O: O.795, P: P.796, Q: Q.797, R: R.798, S: S.799, T: T.800, U: U.801, V: V.802, W: W.803, X: X.804, Y: Y.805, Z: Z.806, A: A.807, B: B.808, C: C.809, D: D.810, E: E.811, F: F.812, G: G.813, H: H.814, I: I.815, J: J.816, K: K.817, L: L.818, M: M.819, N: N.820, O: O.821, P: P.822, Q: Q.823, R: R.824, S: S.825, T: T.826, U: U.827, V: V.828, W: W.829, X: X.830, Y: Y.831, Z: Z.832, A: A.833, B: B.834, C: C.835, D: D.836, E: E.837, F: F.838, G: G.839, H: H.840, I: I.841, J: J.842, K: K.843, L: L.844, M: M.845, N: N.846, O: O.847, P: P.848, Q: Q.849, R: R.850, S: S.851, T: T.852, U: U.853, V: V.854, W: W.855, X: X.856, Y: Y.857, Z: Z.858, A: A.859, B: B.860, C: C.861, D: D.862, E: E.863, F: F.864, G: G.865, H: H.866, I: I.867, J: J.868, K: K.869, L: L.870, M: M.871, N: N.872, O: O.873, P: P.874, Q: Q.875, R: R.876, S: S.877, T: T.878, U: U.879, V: V.880, W: W.881, X: X.882, Y: Y.883, Z: Z.884, A: A.885, B: B.886, C: C.887, D: D.888, E: E.889, F: F.890, G: G.891, H: H.892, I: I.893, J: J.894, K: K.895, L: L.896, M: M.897, N: N.898, O: O.899, P: P.900, Q: Q.901, R: R.902, S: S.903, T: T.904, U: U.905, V: V.906, W: W.907, X: X.908, Y: Y.909, Z: Z.910, A: A.911, B: B.912, C: C.913, D: D.914, E: E.915, F: F.916, G: G.917, H: H.918, I: I.919, J: J.920, K: K.921, L: L.922, M: M.923, N: N.924, O: O.925, P: P.926, Q: Q.927, R: R.928, S: S.929, T: T.930, U: U.931, V: V.932, W: W.933, X: X.934, Y: Y.935, Z: Z.936, A: A.937, B: B.938, C: C.939, D: D.940, E: E.941, F: F.942, G: G.943, H: H.944, I: I.945, J: J.946, K: K.947, L: L.948, M: M.949, N: N.950, O: O.951, P: P.952, Q: Q.953, R: R.954, S: S.955, T: T.956, U: U.957, V: V.958, W: W.959, X: X.960, Y: Y.961, Z: Z.962, A: A.963, B: B.964, C: C.965, D: D.966, E: E.967, F: F.968, G: G.969, H: H.970, I: I.971, J: J.972, K: K.973, L: L.974, M: M.975, N: N.976, O: O.977, P: P.978, Q: Q.979, R: R.980, S: S.981, T: T.982, U: U.983, V: V.984, W: W.985, X: X.986, Y: Y.987, Z: Z.988, A: A.989, B: B.990, C: C.991, D: D.992, E: E.993, F: F.994, G: G.995, H: H.996, I: I.997, J: J.998, K: K.999, L: L.1000, M: M.1001, N: N.1002, O: O.1003, P: P.1004, Q: Q.1005, R: R.1006, S: S.1007, T: T.1008, U: U.1009, V: V.1010, W: W.1011, X: X.1012, Y: Y.1013, Z: Z.1014, A: A.1015, B: B.1016, C: C.1017, D: D.1018, E: E.1019, F: F.1020, G: G.1021, H: H.1022, I: I.1023, J: J.1024, K: K.1025, L: L.1026, M: M.1027, N: N.1028, O: O.1029, P: P.1030, Q: Q.1031, R: R.1032, S: S.1033, T: T.1034, U: U.1035, V: V.1036, W: W.1037, X: X.1038, Y: Y.1039, Z: Z.1040, A: A.1041, B: B.1042, C: C.1043, D: D.1044, E: E.1045, F: F.1046, G: G.1047, H: H.1048, I: I.1049, J: J.1050, K: K.1051, L: L.1052, M: M.1053, N: N.1054, O: O.1055, P: P.1056, Q: Q.1057, R: R.1058, S: S.1059, T: T.1060, U: U.1061, V: V.1062, W: W.1063, X: X.1064, Y: Y.1065, Z: Z.1066, A: A.1067, B: B.1068, C: C.1069, D: D.1070, E: E.1071, F: F.1072, G: G.1073, H: H.1074, I: I.1075, J: J.1076, K: K.1077, L: L.1078, M: M.1079, N: N.1080, O: O.1081, P: P.1082, Q: Q.1083, R: R.1084, S: S.1085, T: T.1086, U: U.1087, V: V.1088, W: W.1089, X: X.1090, Y: Y.1091, Z: Z.1092, A: A.1093, B: B.1094, C: C.1095, D: D.1096, E: E.1097, F: F.1098, G: G.1099, H: H.1100, I: I.1101, J: J.1102, K: K.1103, L: L.1104, M: M.1105, N: N.1106, O: O.1107, P: P.1108, Q: Q.1109, R: R.1110, S: S.1111, T: T.1112, U: U.1113, V: V.1114, W: W.1115, X: X.1116, Y: Y.1117, Z: Z.1118, A: A.1119, B: B.1120, C: C.1121, D: D.1122, E: E.1123, F: F.1124, G: G.1125, H: H.1126, I: I.1127, J: J.1128, K: K.1129, L: L.1130, M: M.1131, N: N.1132, O: O.1133, P: P.1134, Q: Q.1135, R: R.1136, S: S.1137, T: T.1138, U: U.1139, V: V.1140, W: W.1141, X: X.1142, Y: Y.1143, Z: Z.1144, A: A.1145, B: B.1146, C: C.1147, D: D.1148, E: E.1149, F: F.1150, G: G.1151, H: H.1152, I: I.1153, J: J.1154, K: K.1155, L: L.1156, M: M.1157, N: N.1158, O: O.1159, P: P.1160, Q: Q.1161, R: R.1162, S: S.1163, T: T.1164, U: U.1165, V: V.1166, W: W.1167, X: X.1168, Y: Y.1169, Z: Z.1170, A: A.1171, B: B.1172, C: C.1173, D: D.1174, E: E.1175, F: F.1176, G: G.1177, H: H.1178, I: I.1179, J: J.1180, K: K.1181, L: L.1182, M: M.1183, N: N.1184, O: O.1185, P: P.1186, Q: Q.1187, R: R.1188, S: S.1189, T: T.1190, U: U.1191, V: V.1192, W: W.1193, X: X.1194, Y: Y.1195, Z: Z.1196, A: A.1197, B: B.1198, C: C.1199, D: D.1200, E: E.1201, F: F.1202, G: G.1203, H: H.1204, I: I.1205, J: J.1206, K: K.1207, L: L.1208, M: M.1209, N: N.1210, O: O.1211, P: P.1212, Q: Q.1213, R: R.1214, S: S.1215, T: T.1216, U: U.1217, V: V.1218, W: W.1219, X: X.1220, Y: Y.1221, Z: Z.1222, A: A.1223, B: B.1224, C: C.1225, D: D.1226, E: E.1227, F: F.1228, G: G.1229, H: H.1230, I: I.1231, J: J.1232, K: K.1233, L: L.1234, M: M.1235, N: N.1236, O: O.1237, P: P.1238, Q: Q.1239, R: R.1240, S: S.1241, T: T.1242, U: U.1243, V: V.1244, W: W.1245, X: X.1246, Y: Y.1247, Z: Z.1248, A: A.1249, B: B.1250, C: C.1251, D: D.1252, E: E.1253, F: F.1254, G: G.1255, H: H.1256, I: I.1257, J: J.1258, K: K.1259, L: L.1260, M: M.1261, N: N.1262, O: O.1263, P: P.1264, Q: Q.1265, R: R.1266, S: S.1267, T: T.1268, U: U.1269, V: V.1270, W: W.1271, X: X.1272, Y: Y.1273, Z: Z.1274, A: A.1275, B: B.1276, C: C.1277, D: D.1278, E: E.1279, F: F.1280, G: G.1281, H: H.1282, I: I.1283, J: J.1284, K: K.1285, L: L.1286, M: M.1287, N: N.1288, O: O.1289, P: P.1290, Q: Q.1291, R: R.1292, S: S.1293, T: T.1294, U: U.1295, V: V.1296, W: W.1297, X: X.1298, Y: Y.1299, Z: Z.1300, A: A.1301, B: B.1302, C: C.1303, D: D.1304, E: E.1305, F: F.1306, G: G.1307, H: H.1308, I: I.1309, J: J.1310, K: K.1311, L: L.1312, M: M.1313, N: N.1314, O: O.1315, P: P.1316, Q: Q.1317, R: R.1318, S: S.1319, T: T.1320, U: U.1321, V: V.1322, W: W.1323, X: X.1324, Y: Y.1325, Z: Z.1326, A: A.1327, B: B.1328, C: C.1329, D: D.1330, E: E.1331, F: F.1332, G: G.1333, H: H.1334, I: I.1335, J: J.1336, K: K.1337, L: L.1338, M: M.1339, N: N.1340, O: O.1341, P: P.1342, Q: Q.1343, R: R.1344, S: S.1345, T: T.1346, U: U.1347, V: V.1348, W: W.1349, X: X.1350, Y: Y.1351, Z: Z.1352, A: A.1353, B: B.1354, C: C.1355, D: D.1356, E: E.1357, F: F.1358, G: G.1359, H: H.1360, I: I.1361, J: J.1362, K: K.1363, L: L.1364, M: M.1365, N: N.1366, O: O.1367, P: P.1368, Q: Q.1369, R: R.1370, S: S.1371, T: T.1372, U: U.1373, V: V.1374, W: W.1375, X: X.1376, Y: Y.1377, Z: Z.1378, A: A.1379, B: B.1380, C: C.1381, D: D.1382, E: E.1383, F: F.1384, G: G.1385, H: H.1386, I: I.1387, J: J.1388, K: K.1389, L: L.1390, M: M.1391, N: N.1392, O: O.1393, P: P.1394, Q: Q.1395, R: R.1396, S: S.1397, T: T.1398, U: U.1399, V: V.1400, W: W.1401, X: X.1402, Y: Y.1403, Z: Z.1404, A: A.1405, B: B.1406, C: C.1407, D: D.1408, E: E.1409, F: F.1410, G: G.1411, H: H.1412, I: I.1413, J: J.1414, K: K.1415, L: L.1416, M: M.1417, N: N.1418, O: O.1419, P: P.1420, Q: Q.1421, R: R.1422, S: S.1423, T: T.1424, U: U.1425, V: V.1426, W: W.1427, X: X.1428, Y: Y.1429, Z: Z.1430, A: A.1431, B: B.1432, C: C.1433, D: D.1434, E: E.1435, F: F.1436, G: G.1437, H: H.1438, I: I.1439, J: J.1440, K: K.1441, L: L.1442, M: M.1443, N: N.1444, O: O.1445, P: P.1446, Q: Q.1447, R: R
```

故障现象

如图1所示,连接汇聚路由器7708-1的移动MSTP的网终端均可以Ping通137.10.0.70无丢包,但是无法访问137.10.0.70的80端口,显示连接80端口失败即无法上传数据,而连接汇聚路由器7708-2的电信MSTP的网点可以上传数据,但是很慢。

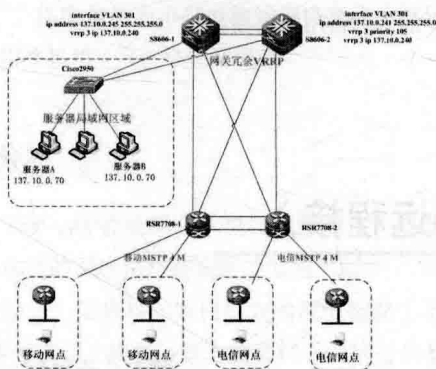


图1 某单位MSTP专线网络拓扑结构

故障排查

由于网点同样访问局域网中服务器C、D等均正常时,第一时间怀疑的是移动的MSTP 4M的线路对访问80端口的局限,在与运营商进行磋商发现MTU等参数没有问题时,排除了运营商的问题。

第二步,详细检查了核心路由和控制列表,由于核心交换机均是双设备双线路冗余,根据此机制,来回路径并不一样,所以笔者第二步怀疑的是来回路径不一致造成数据报文的丢失。为了验证这一问题,在出现故障的汇聚路由器7708-1以太口上直连了一台笔记本电脑配137.10.38.1模拟7708-1下联的移动MSTP的网点,并发起访问服务器A 137.10.0.70的80端口,同时安装了Wireshark抓包软件,抓取了来回的数据包,发现了回来的数据包报RST错误,意味着主机137.10.0.70并没有打开这个80端口。

这个报错非常奇怪,因为137.10.0.70端口的确是打开的。又发现了显示双IP与MAC冲突的报文,这个双MAC是0894.ef0c.fd08和4c11.bf57.e7d2

笔者当时窃喜以为找到原因了,怀疑可能服务器A 137.10.0.70的双网卡浮动的机制导致了某部分数据包访问时打不开80端口。于是致电该服务器的厂家,该厂家的技术人员对此现象也感觉很奇怪,表示的确是双网卡

机制,但是对为什么会造成MAC地址的翻动也很费解。由于该服务器的工作性质是不能中断,导致不能关闭后用其他PC配同样的地址模拟,这就加大了排查的难度。

事已至此,能联想到的原因都一一排查了,笔者并没有放弃。接下来突然出现了一个现象让笔者豁然开朗:这两个翻动的MAC地址并不是同一个厂家的,联想到难道局域网中出现双MAC地址根本不是这台服务器A上面的双MAC,而是存在局域网中服务器B跟服务器A地址一模一样的?如果这样,这一切现象就正常了。

故障排除

立刻登录网络核心交换机上查看MAC地址表,终于发现了真正的原因所在。

7708-1通过核心8606-1上学到的137.10.0.70的MAC地址是不翻动的,一直是0894.ef0c.fd08;而7708-2通过核心8606-2上学到的137.10.0.70的MAC地址是翻动的,当显示0894.ef0c.fd08时,则可以打开137.10.0.70的80端口,当显示4c11.bf57.e7d2时,则无法打开137.10.0.70的80端口。这就是为什么7708-1下的网点一直无法与服务器A传输数据,而7708-2下的网点可以传输数据却很慢的症结。

当找到了局域网中与服务器A同地址的服务器B,把服务器B关机后,一切恢复正常了。笔者费了好大的力气找到了原因,没想到却是其他工作人员简单失误造成的。

故障分析

解决了问题,笔者长舒一口气,从头再梳理下故障的原因:由于局域网中的地址冲突,导致两台服务器地址地址一样,却由于都是Linux系统,并没有任何报错,Ping包均正常。且这两台Linux服务器的网关由于在核心两台8606交换机上做了VRRP的配置,其优先级较高的作为主用网关的核心8606-2能从Linux主机发的免费ARP中识别出目标是虚拟网关的MAC地址,而优先级较低的作为备用网关的核心8606-1不响应Linux主机发出的目标是虚拟网关的MAC地址,这样导致核心8606-1一直学习到137.10.0.70的MAC地址实际上一直是早存在于局域网中的服务器B的。至于服务器A本身的双MAC机制,只是个巧合,并没有造成翻动。

复杂的现象,简单的原因,很多故障隐患就是多个

偶然因素的叠加，最有价值的不是最后的原因，而是发现这个复杂现象真正原因的苦思冥想的排查过程。水落石出，笔者也收获颇丰，再次感受到了网络排查故障的快乐。现娓娓道来，记录下整个过程，与同行分享。

虚拟路由冗余协议

VRRP (Virtual Router Redundancy Protocol, 虚拟路由

冗余协议) 是一种容错协议，也可以叫做备份路由协议。一个局域网络内的所有主机都设置缺省路由，当网内主机发出的目的地址不在本网段时，报文将被通过缺省路由发往外部路由器，从而实现了主机与外部网络的通信。当缺省路由器端口关闭之后，内部主机将无法与外部通信，路由器开启 VRRP 功能后，会根据优先级确定自己在备份组中的角色。优先级高的路由器成为主用路由器，优先级低的成为备用路由器。

端口控制阻碍远程接入

广西柳州 龙志勇

故障现象

一日，财务科人员让笔者帮安装一个应用软件“远程申报系统”，该系统采取 C/S 模式，数据传送至远程服务器，各应用单位安装的是客户端。安装过程非常简单，一会儿就完成了。点击客户端运行，却出现错误提示：“不能连至远程服务器”！检查了网路，这台电脑（下称“申报电脑”）可以连上互联网，因此初步判断问题应该是出在申报电脑上。

故障排查

一般应用软件故障的常用排查方法有：运行环境不符合要求；运行参数设置不对；电脑中毒；安全软件的设置；与其他软件不兼容；操作系统本身的问题。对于此类专用应用软件有相应的运行环境、运行参数设置要求，于是仔细看了附带的软件说明，该软件只要求 32 位的 Windows XP，并能连接互联网就可以了，运行参数已经封装在软件中。申报电脑的运行环境完全符合要求，因此按常规方法继续排查故障。

安装过程中，感到这台电脑的运行速度较慢。于是重启电脑，在安全模式中查杀病毒、木马。经过查杀，确实查出几个木马、病毒，清除后重启电脑，再次运行软件，依然是“不能连至远程服务器”。

本机上装有 360 安全卫士，是不是它阻止了软件的

相关进程？仔细检查了 360 安全卫士的阻止与信任列表，但并未发现软件被阻止，于是干脆把 360 安全卫士卸载，再次重启后运行应用软件，故障依旧。

会不会是其他软件与这远程软件起冲突，导致远程软件不能连到远程服务器？再次重启电脑，进入带网络连接的安全模式，运行软件，还是出现连接错误提示。在此模式下，已经是最小系统了，不会引起软件间的冲突，看来还没有找到故障原因。

申报电脑安装的是克隆版 Windows XP，各版本的克隆系统确实存在差异，这些差异有时候会影响应用软件的运行，但是这种概率很小。在试过多种排查方法未果后，只能试试重装系统了。连换了两个版本的克隆系统来安装，还是不能解决故障。是不是软件设计有问题或者是远程服务器有问题？于是让财务人员打电话询问其他单位的使用情况。得到的回答是其他单位使用正常，都能连接至远程服务器。

无奈之下，只好将软件拿到笔者的电脑（信息科）上安装研究。安装、运行，居然毫无问题，顺利地连接到远程服务器上。检查了一下笔者的电脑，没发现特别的，系统版本和财务科那台电脑一样，运行环境也差不多，这就说明了故障的产生不是由于电脑系统、运行环境产生的。

信息科的端口和财务科的端口分别在 6 号楼层交换机、7 号楼层交换机上。难道是单位网络设置引起的？为

了验证，又到财务科将申报电脑接到财务科的另一条专线上（此专线不接入单位局域网），运行软件，确实没有任何问题，很顺利地就连上了远程服务器。笔者到机房将信息科的电脑的端口跳线接到财务科申报电脑所接的楼层交换机上（7 号交换机），再次运行申报系统，显示不能连接至远程服务器，这证明了问题确实是出在本单位的网络设置上。为了不影响财务科的员工使用“程申报系统”，将账务科的申报电脑的端口跳线接到信息科所接的楼层交换机上（6 号交换机）。

故障分析

为了缩小排查范围，尽快找到故障点，笔者决定先分析本单位的网络拓扑结构图（如图 1 所示）。从网络拓扑图上看到，信息科的端口所在的网络链路（下称链路 1）是 6 号楼层交换机→核心交换机→上网行为管理系统→防火墙→路由器→互联网，财务科的端口所在的网络链路（下称链路 2）也差不多，只是所接的楼层交换机（7 号楼层交换机）不一样。链路 1 和链路 2 相同的部分是从核心路由交换机到路由器，在链路 1 上软件系统可正常使用，说明核心路由交换机到路由器这一部分设备的设置是没有问题的。因此，笔者决定将排查重点放在楼层交换机的设置上。

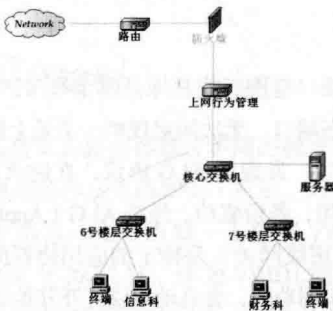


图 1 网络拓扑结构

本单位的楼层交换机和核心路由交换机都是神州数码交换机。登录 6 号楼层交换机，进入特权用户配置模式，使用 show 命令查看配置。6 号交换机的配置非常简单，只是开启了 DHCP，建立了几个 VLAN，并把端口划入了相应的 VLAN 中，并对所有的端口进行简单的流控。又登录 7 号交换机，发现 7 号交换机的配置与 6 号的配置几乎一样，只是管理 IP 和建立的 VLAN 号不一样。反复检查了几次配置，都找不出配置有什么问题。

接着顺着链路依次往上查看各个网络设备的配置，

仍然找不到可疑之处。再次分析单位的网络拓扑图，链路 1 和链路 2 在核心路由交换机上汇聚，链路 1 可以正常使用申报系统，而链路 2 不能正常使用，说明两条链路的公共部分：上网行为管理系统到路由器的设置是没有问题；两个楼层交换机的设置也没有问题，那问题肯定出在核心路由交换机上。

登录核心路由交换机进入特权模式，使用 show 命令仔细地查看配置，当看到这一段配置时，眼前一亮：

```

ip access-list extended hw
...
deny tcp any-source any-destination d-port 4444
deny udp any-source any-destination d-port 5168
deny tcp any-source any-destination d-port 5554
...
```

这一段 ACL 配置的作用是关闭常用的高危端口，以防止一般的入侵攻击。会不会申报系统的远程服务器使用了上述端口？于是在申报系统的安装目录中仔细查看，终于在安装目录中的一个三级子目录下看到一个文件：server.txt，打开一看，文件里列出的是各地区的远程服务器 IP 地址和端口 5168，而端口 5168 却在核心路由交换机中关闭了，所以申报系统肯定是不能使用的。

故障排除

登录核心路由交换机，进入配置模式，使用 no 命令将关闭的端口 5168 重新打开，并将申报电脑所在的交换机端口重新跳回 7 号楼层交换机中。再次在申报电脑运行系统，顺利地连接至远程电脑上。

虽然找到了故障原因并解决了故障，但有一个问题仍感到困惑：为什么 6 号楼层交换机可以运行申报系统而 7 号楼层交换机却不能？进到机房查看，发现 6 号楼层交换机是通过网线接到核心路由交换机的电口，而其他楼层交换机包括 7 号楼层交换机却是通过光纤接到核心路由交换机的光口上。不同的接入方式会不会应用的配置不一样？

于是又登录到核心路由交换机上查看配置，经过仔细查看，发现光口的配置启用了 ACL 控制，而电口的配置却没有启用 ACL 控制，所以导致了 6 号楼层交换机可以连至申报系统的远程服务器上，而其他楼层交换机包括 7 号交换机都不能连至申报系统的远程服务器上。至此，故障原因彻底找到。

经验总结

通过这次故障的排查,笔者深深地感到,作为一名网管,不仅要熟悉网络结构,熟悉各网络设备性能,

还要熟悉各网络设备的配置命令及方法,这样在处理故障时,才能得心应手,事半功倍。

防火墙影响路由备份

▼ 辽宁 岳洁

将路由器配置信息备份到本地计算机的时候,免不了要跨过防火墙。笔者近期使用 TFTP 协议备份路由器数据时,无法连通 TFTP 服务器。备份环境为: Windows XP, Cisco tftp Server, telnet 登录路由器。

故障现象

确定设备连通性没有问题, TFTP 服务已启用(能够正常使用),地址为 192.168.0.16。在计算机 192.168.0.16 上通过 telnet 登录路由器。通过 copy running-config tftp: 命令备份配置,路由器报 %Error opening tftp://192.168.0.16/config (Timed out) 错误, cisco tftp server 内无日志信息。

故障排查

1. 使用命令 netstat -na, 查看是否在监听 UDP69 端口, 已经监听。
2. 检查备份命令未出错。使用 TFTP.exe 命令行方式查看服务已经启动。
3. 使用相同环境备份局域网内其他设备, 备份成功。

经过以上的操作对比发现,是备份经过防火墙的数据时失败。询问防火墙管理员 TFTP 是否开放,回复已经开放。

再次检查备份过程,无误;还是怀疑防火墙问题。于是,在防火墙上将 192.168.0.16 与路由器点对点打开所有服务,备份成功。断定防火墙配置规则有误。

经查找防火墙不计其数的规则发现,配置 TFTP 服务内 69 端口类型选择为 TCP,立即更改为 UDP,本以为这就是问题所在,此时备份配置依然显示 %Error opening

tftp://192.168.0.16/config (Timed out) 错误,但在 cisco tftp server 内出现显示 receiving 'config' file from 192.168.0.1 in binary mode

Failed (timeout error), 查找备份的文件大小为 0。

看来更改防火墙策略的总方向是对的,我就想 TFTP 是建立了连接,可是在数据传输过程中出现了问题,从而导致了失败,应该是还有别的端口或者协议需要开启。既然 TFTP 协议使用的是 UDP 端口,索性将点对点的 UDP 的端口全开放,果然备份成功。

故障排除

后缩小端口范围想找具体是哪个端口,经测试发现使用的是动态端口,无法固定规则。于是上网查找 TFTP 使用动态端口,发现了 ALG 协议,在防火墙上将选项 ALG 一项启用,备份成功。经查 ALG (Application Level Gateway, 应用级网关) 是特定的应用协议的转换代理,开启应用层识别功能,会自动协议打开其他必需的端口。

经验总结

1. 当怀疑是防火墙配置的问题时,可以点对点开启所有服务测试,但一定要恢复正常端口配置。
2. 防火墙规则设置不可草率行事,要依据一定之规,否则在查找配置规则困难。
3. 除了 TFTP 协议要使用 ALG 动态端口解析外,还有以下协议也需要使用: DNS、FTP、H.323、HWCC、ICMP、ILS (Internet Locator Service)、NetBIOS。

VRRP 引发网络中断

福建泉州 王刚 叶永安 曾玮琳

随着网络的快速普及和相关应用的广泛部署,对基础网络的可靠性要求越来越高,网络的可靠性也成为用户最关注的焦点。VRRP (Virtual Router Redundancy Protocol, 虚拟路由冗余协议) 目前已经得到非常广泛的应用, VRRP 是一种容错协议,能够确保个别路由设备在出现故障后,能够选举新的网关设备承担数据流量和负载均衡,确保数据在传输过程不中断。该协议通过把多台路由设备整合成一台虚拟的路由设备,将虚拟路由设备的 IP 地址作为用户的默认网关实现与外部网络通信。其外在表现是,在客户端计算机虽然也需要配置 1 个网关才可以实现上网,而实际这个网关是虚拟网关,该网关是由两台或多台路由设备再使能了 VRRP 协议后虚拟生成的网关。VRRP 协议在确保网络通畅方面发挥了很重要的作用,但在实际应用中,因网络链路、端口阻塞、配置不当等原因极易造成客户端用户上网中断。

故障网络拓扑结构

单位有两台华为路由器通过不同的物理链路连接外部网络,其网络拓扑示意图如图 1 所示,两台路由器均配置了 VRRP 协议。在路由器一上建立 VRID1,设置其虚拟 IP 地址为 20.1.1.11,作为 VRID1 的主用设备,同时设置其为 VRID2 的备用设备。在路由器二上建立 VRID2,设置其虚拟 IP 地址为 20.1.1.12,作为 VRID2 的主用设备,同时设置其为 VRID1 的备用设备。内部网络中有部分客户端使用路由器一作为网关,有部分客户端使用路由器二作为网关,两台路由器均采用 VRRP 的缺省参数,两台路由器均配置了 OSPF 路由协议。

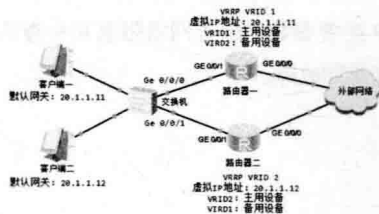


图 1 网络拓扑示意图

相比一主一备的 VRRP 方式,多网关负载分担其优点是可以实现流量的负载均衡,两台路由器均参与流量转发,缺点是增加了路由器的运算负荷,但负荷增加不多,一般网络都会采用多网关负载分担方式。内部网络客户端可以根据需要通过设置不同的网关访问外部网络。

故障现象

路由器一和路由器二 VRRP 协议配置完成,两台路由器的 VRRP 状态极不稳定, VRRP 状态不停地在 Backup、Master 两种状态中切换。内部网络与外部网络通信异常,丢包率高达 50%,无法正常访问外网,而丢包发生在路由器在主备切换时。

故障原因分析

1. 链路故障

当 VRRP 状态不稳定时,由链路引发的可能性最大,当链路状态出现故障后,使用 VRRP 协议的路由器之间就接收不到主备之间的 VRRP 参数或接收到 VRRP 参数的时间超过了配置的主备切换时间,路由器的 VRRP 的主备也会自动切换。这一般是由于链路接头连接不紧密或链路损耗大造成的。

2. 网络阻塞

网络阻塞一般是由于病毒或广播风暴造成,也有可能是路由器部分运行协议数据包过多造成,在网络比较拥塞的环境下,Backup 路由器可能在等待超时后才收到 Master 路由器的报文,导致备份组内的成员频繁的进行主备状态转换。在网络比较拥塞的环境,可以适当增加 Backup 等待延迟时间。

3. CPU 占用率高

使用相关命令查看处理 VRRP 协议报文互通的业务板和路由器 CPU 占用率是否过高。如果 CPU 占用率过高,会造成部分 VRRP 报文无法及时处理或者被丢弃,也会

引发路由器 VRRP 协议主备频繁切换。

4. 配置故障

这里说的配置故障，不仅仅是 VRRP 参数配置错误的问题，路由器其他运行参数配置错误也会引发了 VRRP 故障，因为其他运行参数在设置完成后，最后再设置 VRRP 参数的话，很可能会造成 VRRP 无法正常运行，这种故障比例也是很高的。而配置 VRRP 参数错误的比例反而不高，配置 VRRP 一般只要虚拟 IP 地址、VRRP 广播报文间隔时间、双方认证方式和认证关键字相同就可以了。而由于 RIP、OSPF 等路由协议、STP 协议等引发故障的比例反而较大，这类故障比较难以发现和排除。

故障排除

1. 检查两台路由器 VRRP 配置参数是否一致

经过检查发现双方路由器 VRRP 参数设置均一致，很多参数都采用了默认参数，故障不是由于 VRRP 配置参数设置错误引发。

2. 检查 CPU 占用情况

进入路由器全局模式，使用 `display cpu-usage` 命令查看 CPU 占用率，发现路由器和处理 VRRP 协议的背板 CPU 占用率处于正常状态。

3. 检查链路

在路由器一内使用 Ping 命令分别在路由器二的连接端口之间、路由器一对内部网络和路由器一对外部网络之间进行测试，发现路由器之间、路由器一至外网之间的 Ping 包均正常，路由器至内网有部分 Ping 包丢失，看来链路有故障点。检查路由器一连接内部的情况，发现路由器连接交换机的水晶头连接不太紧密，重新制作了水晶头后，再从路由器一向内部进行 Ping 操作，未出现丢包现象，但路由器 VRRP 主备切换仍在频繁发生，看来故障也不是链路问题引发。

4. 检查网络阻塞

进入路由器全局模式，使用 `display interface` 命令分别查看路由器各端口的数据信息，发现各端口有错误报文，但均属正常范围。为确保检查的正确性，分别对路由器一的内网连接端口进行了流量抓包分析，发现路由器会出现周期性大流量现象，可能会出现短暂阻塞，但这些数据流量属正常业务流量，同时也发现出现 MAC 地

址漂移现象，也出现少量广播包，网络中可能出现网络环路。检查发现，有多位内网办公用户使用笔记本电脑办公，因工作需要，需要在多台交换机上移动办公，造成出现 MAC 地址漂移现象，故障也不是因阻塞引发。

5. 检查路由器其他的运行参数

看来 VRRP 出现主备频繁切换是由其他路由器运行参数引发的。使用命令 `display stp brief` 命令查看两台路由器互连端口的 STP 状态，发现 STP 状态正常。使用 `display arp` 命令查看两台路由器是否成功学习到下挂设备的 ARP 表项，通过对比发现 ARP 表项正确。使用 `display ospf routing` 命令分别查看两台路由器，发现路由条目基本正常，故障也不是由于路由器其他运行参数配置错误引发。

6. 在路由器上打开 VRRP 报文调试开关

使用 `debugging vrrp packet` 命令打开 VRRP 报文调试开关，经过数据包的分析发现 VRRP 运行基本正常，发现 VRRP 协议运行未出现异常。

7. 抓包分析

在故障排除未果的情况下，笔者怀疑可能是外部网络路由的问题，遂对两台路由器的连接外网的端口进行抓包分析。通过对比，发现两台路由器在外网端口接收到的网络数据流量存在问题。后经协调，查看了外部网络中连接两台路由器的路由器的路由表，发现到外网路由器至内部网络有 2 条等价路由，其中一条下一跳指向路由器一，另一条下一跳指向路由器二。由于存在两条等价路由，当外网路由器回应至内部网报文时，依照负载均衡分担原则，数据流会交替从路由器一和路由器二进行转发。当路由器接口出现短暂阻塞或链路出现故障时，VRRP 会进行主备切换，当完成切换时，OSPF 还未删除至不用的路由器的路由条目，但报文仍然交替转发，从而出现流量中断。经协调，在路由器一和外网路由器上各增加了一条静态路由，故障排除。

经验总结

当 VRRP 出现故障时，特别是出现主备切换频繁时，可采用先硬后软，先简后繁的方式，一般按照检查链路，检查 VRRP 配置参数，检查网络阻塞和检查其他路由协议的流程来排除故障。

A large, stylized white globe graphic is positioned on the right side of the cover, spanning across the top and bottom sections. It features a circular outline with several curved lines representing latitude and longitude.

NetAdmin World 2017

第 4 章 信息安全

防共享，堵漏洞

广东 黄国贤 叶世青

防共享检测技术介绍

目前市面上有很多的防共享设备，其主要检测原理大约如下：

1. Flash cookie 技术原理

FLASH COOKIE 是由 FLASHPLAYER 控制的客户端共享存储技术，它具备以下特点：类似 HTTPCOOKIE，FLASHCOOKIE 利用 SHARED OBJECT 类实现本地存储信息，SHARED OBJECT 类用于在用户计算机上读取和存储有限的数量，共享对象提供永久贮存在用户计算机上的对象之间的实时数据共享；本地共享对象是作为一些单独的文件来存储的，它们的文件扩展名为 .SOL。默认状态下，它们的尺寸一般不超过 100KB，并且不会过期，这一点与传统的 HTTP COOKIE 不同（4KB）；本地共享对象并不是基于浏览器的，所以普通的用户不容易删除它们。这使得本地共享对象能够长时间的保留在本地系统上。

由于 FLASHCOOKIE 具有可操作性、比普通 HTTPCOOKIES 有着更大存储空间、更好的隐蔽性等优点。加上现在 FLASHPLAYER 已经成为互联网用户标配之一，不存在兼容性的问题，因此它非常适合用来保护客户端数据、收集用户行为等。当用户使用 IE 访问某个 FLASH，防共享设备会预先判断浏览器是否存在 FLASH COOKIE 值，如果没有将会种植 FLASH COOKIE 值为 A，如果存在 FLASH COOKIE 值则进行记录；用户使用不同浏览器打开访问网站时，FLASH COOKIE 值都会进行共享，因此不会引起误判；当缓冲区中发现存在两个不同的 FLASH COOKIE 值时，则将被判断为代理共享上网，从而对其进行封堵并进行定向页面提醒。

2. 多应用特征检测

设备中内置防代理软件规则库，对最新的热门软件唯一特征库进行识别。

终端使用这些应用后，在使用该软件或者该软件进行升级更新时，设备在网络出口处都能检测到来自于该 IP/ 用户的应用特征。若发现有同一个用户账号下有两

个或超过两个的 IP/ 用户接入，则可判断其为共享上网的行为，并自动检测到有两个或超过两个终端的接入数量。

3. 时间戳算法检测

对付病毒最好的办法就是使用杀毒软件，在 WINDOWS 中可选的杀软种类有很多，其中比较著名的杀毒软件有卡巴斯基、F-SECURE、MACFEE、诺顿、趋势科技、熊猫、NOD32、AVG 以及 F-PORT 等等。安装配置和使用都比较方便。

根据 RFC791-IP 包格式规范，IP 包扩展属性中有 2 字节的 IDENTIFICATION（简称为 IP_ID），WINDOWS 用户的 IP_ID 随着用户发送的 IP 包数量而线性增加（无论 IP 包发送到何处，包括发给自己）WINDOWS 95/98，每发一个 IP 包，IP_ID 增加 256；WINDOWS 2000/NT/WINDOWS XP/WINDOWS 7/WINDOWS 8，每发一个 IP 包，IP_ID 则增加 1，如图 1 所示。

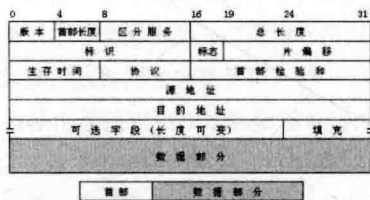


图 1 IP 包格式

根据以上特性，同一主机（使用 WINDOWS 操作系统）ID 字段随着用户发送 IP 数据报文而线性增加（每包增加 1 或 256），不同的主机的 IP 报文中的 ID 字段随着用户发送数据报文而形成各自的轨迹。共享接入用户的上网请求时间以及对应主机的发包频率是不可能完全一致的，所以可以利用该特性做共享接入行为的检测以及同时在线主机数的精确判定。

假设某时刻、来自某个源 IP 在一段时间内数据报文中 ID 字段形成三条直线，可初步分析该 IP 下有三台主机同时上网。

4. 利用 User Agent 检测

USER-AGENT 是 HTTP 协议中的一部分,属于头域的组成部分,USER AGENT 也简称 UA。较为普通的一点来说,是一种向访问网站提供你所使用的浏览器类型、操作系统及版本、CPU 类型、浏览器渲染引擎、浏览器语言、浏览器插件等信息的标识。UA 字符串在每次浏览器 HTTP 请求时发送到服务器。利用 USER AGENT 可以用来识别浏览器名称、版本、引擎以及操作系统等信息的内容。

以上 4 种检测方法是业界较为新的检测模式,当然好的防共享设备肯定是结合多项检测技术如 ID 轨迹检测、流量/连接数统计或 MAC 地址检测等这些传统的办法一起使用,以防止误判。

防共享设备的部署

以校园网建设为例,某学校目前总共 1 万人左右,因为此次部署防共享主要针对学生上网,所以教学楼、老师宿舍暂时不部署。学生宿舍楼每层都一个接入交换机,在通过综合布线到学生宿舍,而在每栋 1 楼进行二次汇聚后上联到核心交换机,此次部署的防共享设备主要在核心汇聚交换机和 BRAS 之间,具体主网如图 2 所示。

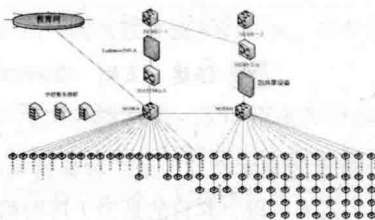


图 2 某大学组网图

在部署之前,该大学只有缴费宽带用户数约为 2000 左右,占比不到 20%,一拖 N 给校园网的运行带来了如下问题:用户投诉增多,主要反映网速慢,原因学生共享上网、P2P 等多线程下载造成,很多学生自己架设的无线网络被蹭网都不知道;用户流失严重,为了给学生提供好的良好的宽带体验,每年学校在设备维护、更新换代以及带宽出口扩容等方面需要投入大量的资金,而一拖 N 造成用户流失严重,无法实现“以网养网”的目的;一些共享的网络甚至会被盗用进行一些网上违法行为,从而造成宽带报装学生需要承担相应的法律责任,却无法追溯到真正的违法者和保护合法的使用者的权益。另外学校也要承担相应的连带法律责任。

部署之后,通过防共享设备后台管理程序可以了解到:

1. 经过近两周的采集,学校最高峰时有 6523 个用户接入校园网,如图 3 所示,可见在校园 1 拖 N 现象比较严重,造成大量学生未交费使用校园网。



图 3 捕获终端数

2. 一周的上网应用流量排行,通过应用流量的排名分析,WEB 流媒体占比最高,达到 26.85%,接下来为 HTTP 的网站访问占比达到 29.83%,P2P 流量:16.22%,所以原先认为学校流量占比最高为 P2P 下载的猜想是错的,为了分流 WEB 流媒体,提高学生业余时间的在线视频的观看感知和节约出口带宽,在校园网内建设 VOD 视频点播系统还是有必要的。具体流量排名如图 4 所示。



图 4 一周用户流量分布

3. 根据国家对于互联网信息安全要求的规定,防共享系统可以对学生上网访问行为进行记录,供日后审计溯源用,如图 5 所示。

序号	IP地址	用户名	设备类型	设备地址	URL地址	访问时间	备注
1	10.10.10.1	张三	台式机	10.10.10.1	http://www.baidu.com	2019-11-01 10:00	
2	10.10.10.2	李四	笔记本	10.10.10.2	http://www.qq.com	2019-11-01 10:05	
3	10.10.10.3	王五	台式机	10.10.10.3	http://www.163.com	2019-11-01 10:10	
4	10.10.10.4	赵六	笔记本	10.10.10.4	http://www.sina.com	2019-11-01 10:15	
5	10.10.10.5	孙七	台式机	10.10.10.5	http://www.126.com	2019-11-01 10:20	
6	10.10.10.6	周八	笔记本	10.10.10.6	http://www.189.com	2019-11-01 10:25	
7	10.10.10.7	吴九	台式机	10.10.10.7	http://www.21cn.com	2019-11-01 10:30	
8	10.10.10.8	郑十	笔记本	10.10.10.8	http://www.360.com	2019-11-01 10:35	

图 5 上网行为日志

4. 带宽智能管控:可以根据不同的业务应用、路由出口、用户名和时间段进行出口带宽的灵活设置,从而保证学校师生的互联网使用达到可控可管的地步,如图 6 所示。

图 6 带宽分配

5. 防共享设备可以对共享接入的配置进行灵活设置,如可以根据 PC、移动终端达到多少数量后进行启动、冻结时长多久等,如图 7 所示。

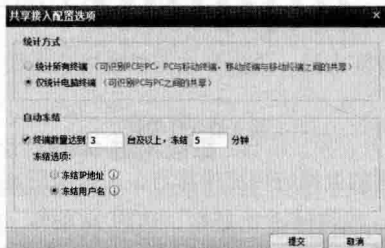


图 7 防共享接入设置

结语

通过部署防共享设备,之前忧虑的问题得到一一解决,并且通过内容、账号、时段、日志和出口带宽等多个方面来对网络进行控制,实现了校园网络可控可管。并且通过防共享设备实现了禁止一拖 N 现象,让真正的缴费者享受高速的网络,让“以网养网”的目标得以实现。希望本文中关于部署防共享设备的方法和想法对在建设和维护校园网时能起到一定作用。

正确使用 Cookies

福建 王刚 曾玮琳 郑洪飞

现在上网很多网站都需要用户注册,不然很多需要权限的资源就无法访问,在注册成功并登录后,在一定的时间内,用户无需重新登录仍可访问相应权限的资源,这些网站会自动识别和记录用户信息,实现这个功能的就是 Cookies, Cookies 会记录用户的访问时间、访问页面和每个浏览过的网页驻留时间等信息,这些网站会根据用户的浏览资源提供相应的个性化服务,例如会自动推荐一些相关联的资源等,还会根据用户浏览的习惯和各类统计信息来完善网站功能等,但 Cookies 在提高用户上网体验和方便的同时,也存在一定的安全隐患,极易泄露用户的个人隐私,正确使用 Cookies 功能且确保 Cookies 安全,不泄露用户个人信息就显得尤为重要。

Cookies 及其功能

Cookies 是存储在用户计算机内,记录用户浏览相

关网站用户信息的文本文件,是一种保持 Web 应用程序执行状态的技术手段,其目的是为了帮助相关网站记住用户信息状态。

用户使用不同的浏览器访问网站时, Cookies 会存储在相应浏览器的文件夹内,同时,会以用户访问网站的域名为名称生成相应的文件夹。可以将 Cookies 看成不同的“仓库”,“仓库”内有很多的“房间”,这些“房间”内存放的就是用户信息,“仓库”因用户使用浏览器的不同,其“物理位置”也会不同,“仓库”内“房间”的名称就是用户浏览相应网站的域名。用户在浏览相应网站时,网站服务器不仅会反馈给用户相应浏览网页,也会根据用户相关信息反馈一个包含有时间、日期等相应信息的 Cookies,并将之存储在用户的硬盘上, Cookies 信息会在网站服务器和用户浏览器之间进行传递,不同浏览器和不同网站之间的 Cookies 不会彼此覆盖。之后,当该用户再次访问网站时,浏览器会在用户

硬盘 Cookies 文件夹内查找与该网站相关联的 Cookies，如果该 Cookies 存在，那么浏览器便会将该 Cookies 和网页请求一起发送到网站，如图 1 所示，为使用 IE 浏览器查看 Cookies 信息的方法。当然，并不是所有的浏览器都将 Cookies 信息放在文本文件中，比如有的浏览器则是将 Cookies 信息存储在注册表中。

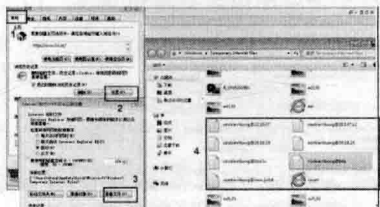


图 1 使用 IE 浏览器查看 Cookies 信息

Cookies 的主要安全隐患

Cookies 有许多安全隐患，其中极易造成用户信息丢失的安全隐患主要有 3 点：

一是 Cookies 本身容量不足而易溢出。目前大多数浏览器最大仅支持 4096 字节的 Cookies，同时还限制了存储的 Cookies 数量，如果要存储更多数量的 Cookies，较早的 Cookies 便会被丢弃，所以当在使用 Cookies 时，特别是用户访问网站数量较多的时候，非常容易丢失关键网站的 Cookies。

二是易遭受 XSS 攻击。XSS 攻击为跨站脚本攻击，经常用来攻击存在 XSS 漏洞的用户和服务器，它允许恶意 Web 用户将代码植入到提供给其它用户使用的页面中，即攻击者可以把自己的代码越过安全边界线注射到另一个不同的、有漏洞的 Web 站点中，当这些注入的代码作为目标站点的代码在受害者的浏览器中执行时，攻击者就能窃取如用户网银、各类管理员帐号等各类敏感信息，可以读取、篡改、添加、删除企业敏感信息和钓鱼欺骗用户、在网站上挂木马等，其攻击过程如图 2 所示。

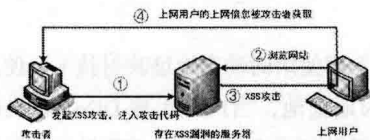


图 2 XSS 攻击过程

三是 Cookies 不能即时清除问题。因为 Cookies 有一定的生存周期，当用户 A 在使用自己的帐号上网后，有些信息还会驻留在计算机内，当后面的用户上网时，

就会使用用户 A 的信息上网，这样就会出现用户 A 的信息被后面的用户冒用的现象，甚至做一些非法的操作等，特别是在网吧等公共场所上网或一机多用户操作时，就会给某些用户造成一定的个人信息泄露的损失，这也是 Cookies 的一个弊病，即在退出浏览器后，很多 Cookies 的信息不会被即时清除。

确保 Cookies 安全措施

一是做好 XSS 漏洞防御。现在 XSS 漏洞已经很少，用户需要及时升级自己上网所使用的浏览器版本，较旧版本的浏览器还不能很好地防御 XSS 漏洞。此外，XSS 漏洞是利用了 Web 页面的编写不完善来进行攻击的，用户可以使用安全软件对包括 URL、查询关键字、HTTP 头、POST 数据等在内的提交信息进行可靠的输入验证，仅接受指定长度范围内、采用适当格式、采用所预期的字符的内容提交，对其他的一律过滤，对包括 Session 标记或者 HTTP 引用头进行检查，以防 Cookies 被第三方网站所执行等。

二是定期清理 Cookies。清理 Cookies 不仅可以清理系统上网垃圾，提高系统运行速度，还可以保证用户的上网信息不被泄露，用户必要养成定期清理 Cookies 的习惯，可以手动清除，也可以选择工具软件进行清除，清理 Cookies 虽然不能百分百的解决安全隐患，但可有效预防 Cookies 可能造成的安全隐患。当 Cookies 是在文件夹时，以 IE 浏览器为例，清除 Cookies 的方法如图 3 所示。也可以使用图 1 的方法，找到各 Cookies 文件，将其删除。



图 3 清理 Cookies 方法

对于 Cookies 在注册表中的清除方法如下（如图 4 所示）：在 Windows 操作系统中运行“Regedit”，找到如下键值：HKEY_LOCAL_MACHINE/Software/Microsoft/Windows/CurrentVersion/InternetSettings/Cache/SpecialPaths/Cookies，这是 Cookies 存留在内存中的键值，只要把这个键值删除即可。



图4在注册表中清除 Cookies 方法

三是必要时可以禁用 Cookies 或提高 Cookies 的安全级别。通过禁用 Cookies、开启 Cookies 安全警告或每次访问后删除与操作相关的 Cookies 方式防范跟踪 Cookies，这里以 IE 浏览器为例，禁用 Cookies 方法和提高 Cookies 的安全级别如下（如图 5 所示）：打开“工具/Internet 选项”中的“隐私”选项卡，调整 Cookies 的安全级别。通常情况，可以调整到“中高”或者“高”的位置即可，也可以将安全级调到“阻止所有 Cookies”。如果只是为了禁止个别网站的 Cookies，可以单击“编辑”按钮，将要屏蔽的网站添加到列表中。在“高级”按钮选项中，可以对第一方 Cookies 和第三方的 Cookies 进行设置，第一方 Cookies 是用户浏览网站的 Cookies，第三方 Cookies 是非正在浏览的网站发给用户的 Cookies，通常要对第三方 Cookies 选择“拒绝”，目前主流的浏览器都有禁止第三方 Cookies 的功能。若没有此项功能的浏览器，用户可以通过安全防护软件来防范跟踪 Cookies。这里需要说明的是，禁止 Cookies 或

提高 Cookies 安全级别虽然可以增强用户上网的安全级别，但也有可能会造成一些弊端或降低用户的上网体验，比如在一些需要 Cookies 支持的网站里，会发生一些莫名其妙的错误，如无法打开部分文件或不能使用包括免费电子邮件在内的某些网站功能等，所以笔者建议用户可以对上网的部分安全网站进行筛选。



图5禁用和提高 Cookies 方法

四是养成一个良好的上网习惯。不要在一些来源不明的网页上填写任何有关个人的隐私信息，特别是一些重要和敏感的信息，以免泄漏用户个人信息从而造成一些不必要的损失。例如在打开一些网站时，可以通过网站的信息来查看网站是否合法，合法的网站其安全性一般都值得信任和有保障的。一般合法的网站在网站的最下方有类似“京 ICP 证 032616 号”的网站信息，然后在搜索网站中搜索关于“国家工信部网站备案查询”，找到“工信部”主页，在主页中找到公共查询的入口，可在其中查询用户上网的网站是否合法。

IP 地址封堵有法

广东 米九

笔者工作的单位最近发现内网有计算机感染病毒，这些计算机是可以访问互联网的，通过分析日志发现感染病毒的电脑不停地和互联网的某些 IP 地址建立连接。单个内网的 IP 建立的连接数达到了几十万，这是很不正常的现象。理论上，内网的一个 IP 地址不可能有这么大的连接数，因为我们内部网络管理屏蔽了部分下载软件，鉴于此，我们判断是内网的部分计算机被控制，对互联网发起了 DDos 攻击。内部网络的简要拓扑图如

图 1 所示。

防火墙上使用的动态地址映射技术，使用了四个公网 IP 作为地址池，当内部出现 DDos 攻击时候，防火墙出现大量的新建会话，另外需要处理这些无应答的请求，CPU 的利用率会不断地上升。面对这样大的攻击流，防火墙的资源被大量占用，出现一个明显的问题是 Web 管理界面响应变得非常缓慢，点击一个按键半天都没有反应。

通过 SSH 登录到防火墙上，使用命令 `clear session` 尝试清除所有的会话，但是效果并不理想，因为刚清除的 IP 地址的会话又会马上建立新的 session，必须要找到攻击的源头进行封堵才能解决问题。通过旁路抓包分析，结合防火墙的会话日志，发现可疑的 IP 地址有三个，分别是 192.168.1.3、192.168.3.8、192.168.7.10，这些 IP 地址发出大量的数据包，在防火墙上建立的连接数都达到数十万，必须对其进行封堵，下面介绍一下常用的三种封堵的办法。

方法一：直接在三层网关设备上面进行封堵。

这种方式总结为野蛮模式的封堵，就是以封堵为大前提，牺牲小部分用户保住整体网络。内部局域网都是划分 Vlan 网段的，把 192.168.1.3、192.168.3.8、192.168.7.10 对应的 Vlan 找出来，直接 `interface Vlan ID` 然后再输入 `shutdown` 命令，这是最快捷的方式，比拔网线还高效率，但是很自然地被 shutdown 的 Vlan 整个网段的 IP 都无法访问了，等于是消失在局域网中，攻击的源头自然就会被封堵。接下来就是发通知，找到那几台 IP 对应的机器进行网络隔离，再把 shutdown 的 Vlan 重新启动。

方法二：在防火墙上使用添加黑名单的方式进行封堵。

这种方式是利用防火墙的黑名单功能，建立策略将匹配规则的 IP 地址进行封堵。简要的配置命令如下：

```
exec block-ip add ip192.168.1.3 timeout 600
exec block-ip add ip192.168.3.8 timeout 600
exec block-ip add ip192.168.7.10 timeout 600
```

命令的意思是将 192.168.1.3、192.168.3.8、192.168.7.10 放进防火墙的全局黑名单，放置的时间是 600 秒钟，这段时间内上述的 IP 地址发起的请求将被阻止，不会产生新的 session。实际上病毒感染的电脑还是会不断地发起建立连接请求，流量还是会流向防火墙，

只是设备将不会响应黑名单里的请求。

方法三：使用黑洞路由，添加一条路由指向 NULL 0 接口。

如图 1 所示，核心层的交换机与汇聚层的设备通过 OSPF 路由协议互联，所以在核心层建立一条黑洞路由就能使全网学习到。简要配置如下：

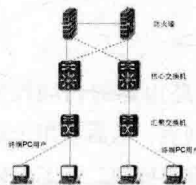


图 1 内部网络简要拓扑图

```
Ip route-static 192.168.1.3 255.255.255.255 NULL 0
description bingdu
```

```
Ip route-static 192.168.3.8 255.255.255.255 NULL 0
description bingdu
```

```
Ip route-static 192.168.7.10 255.255.255.255 NULL 0
description bingdu
```

Null 0 接口是一个永远不会 down 的接口，它的配置命令跟静态路由差不多，实现起来较为简单，最后面加上描述信息用于标记此路由条目。这样能把感染病毒的 IP 指向了一个黑洞，请求不会到达防火墙也不需要再在防火墙上添加策略封堵，能减轻防火墙的负担。

综上所述，对于局域网内部的 IP 地址封堵，可以结合多种方式进行，最理想的状态是在接入端着手，从最靠近攻击源头的设备将流量进行阻塞，若出现多个不同网段的 IP 发起攻击，使用 shutdown Vlan 的方式就比较困难，个人建议是先编辑好一个黑洞路由的脚本，只要把封堵 IP 地址都写上，直接在交换机上面粘贴配置，这样的方式效果又快又明显。

华为 S9306 的访问控制

深圳 李发成

Cisco 交换机、路由器的访问控制过程比较简单，首先定义访问控制列表，然后应用于端口即可。可是有些华为交换机配置有点麻烦，且不太好理解。本文以华为 S9306（如图 1 所示）为例来说明其配置过程。

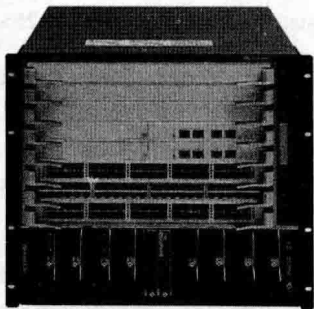


图 1 华为 S9306

配置步骤分别是定义访问控制列表、创建流分类、定义流行为、创建流策略和应用流策略。只有定义好了这五个步骤，才能使定义的访问控制列表生效起作用。

例如学校教室监控，班主任可以在自己的计算机上安装客户端，通过给定的用户名和密码在线浏览和录像回放教室前后的监控数据。虽然有用户名和密码，但其他人如果知道用户名和密码，也是可以访问的。比如有一个班主任就把客户端软件、用户名和密码都给了一个家长，原因是这个家长想通过手机随时查看自己的小孩上课的表现情况。但这是不被允许的，当学校知道后要求通过对此进行技术性限制，因为修改密码后仍然有可能被泄漏。ACL 可完全杜绝非法访问，通过定义 ACL 只允许某些 IP 访问某些监控。

假设我们只允许在学校局域网内访问监控数据，学校办公子网分别有 219.223.116.0/24、219.223.117.0/24、219.223.118.0/24 和 219.223.119.0/24，汇聚合并为 219.223.116.0/22，其中教室监控子网为 172.16.88.0/24，定义原地址为 219.223.116.0/22，目的地址为 172.16.88.0/24 的扩展访问控制。以下本文中的 IP 地址不代表真实的 IP。

定义访问控制列表 ACL

acl number 3401（这里使用高级访问控制，所以 ACL 编号从 3000 开始）

```
rule 10 permit ip source 219.223.160.0 0.0.3.255
destination 172.16.88.0 0.0.0.255
```

```
rule 20 deny ip source any destination 172.16.88.0
0.0.0.255
```

其中办公子网掩码为 22 位，应用于 ACL 中的反掩码为：

```
00000000.00000000.00000011.11111111=0.0.3.255。
```

创建流分类

创建一个流分类，并进入流分类视图，流分类名称假设为“3401”，可以是任何一个有效的命名，默认情况下流分类之间是“逻辑或”关系，即报文只需匹配流分类中的一个规则即可，优先级默认为 5，配置结果如下：

```
traffic classifier 3401 operator or precedence 5
if-match acl 3401
```

创建流行为

创建一个流行为，进入流行为视图，行为名称为“3401”，其动作有两个：deny 或者 permit，如果配置了 deny 动作，则符合流分类规则的报文都会丢弃，所以不能再配置其它动作。如果配置了 permit 动作，则对符合流分类规则的报文采取的动作进行逐条匹配。

```
traffic behavior 3401
permit
```

创建流策略

很创建名为“3401”的流策略并进入流策略视图，

在策略中关联流分类和动作。

```
traffic policy 3401
classifier 3401 behavior 3401
```

应用流策略

在全局出方向应用流策略

```
traffic-policy 3401 global outbound
```

华为网络设备是通过流分类、流行为、流策略进行访问控制的，如有另外的安全要求，只需要修改访问控制列表中的内容，而无需更改流分类、流行为和流策略中的内容即可。



IP 扩展访问控制列表的配置

甘肃 左振辉

本文讨论利用 IP 扩展访问控制列表来实现网络应用服务访问控制的配置方法（采用 Cisco 设备）。

扩展访问控制列表配置方法

在全局模式下建立扩展访问控制列表，配置如下：

```
Router (config) #access -list access-list-number
{permit|deny}protocol source source-wildcard [operator
port] destination destination-wildcard [operator port]
```

以上中的“access-list-number”对 IP 扩展访问控制列表范围是 100-199 和 2000-2699。不同类型访问控制列表列表号如图 1 所示。

访问控制列表类型	列表号	
IP	标准的	1-99,1300-1999
	扩展的	100-199,2000、-2699
	命名的	名字(OS11.2 版本以上可用)
AppleTalk		600-699
IPX	标准的	800-899
	扩展的	900-999
	SAP 过滤的	1000-1099
	命名的	名字(OS11.2 版本以上可用)

图 1 列表类型和对应的列表号

而“permit”或者“deny”关键字可以指定哪些匹配访问控制列表语句的报文是允许通过接口或被拒绝通过。该选项所提供的功能与标准 IP 访问控制列表相同。

“portocol”即协议表项定义了需要被检查的协议，例如 IP、TCP、UDP、ICMP 等。协议选项是很重要的，因为在 TCP/IP 协议簇中的各种协议之间有密切关系。如 IP 数据包可用于 TCP、UDP 协议及各种路由协议的传输，如果指定 IP 协议，访问控制列表将只检查 IP 数据包进行

匹配，而不再检查 IP 数据包所承载的 TCP、UDP 等上层协议。如果根据特殊协议进行报文过滤，就要指定该协议。此外，应将更具体的表项放在访问控制列表靠前的位置。例如，如果允许 IP 地址的语句放在拒绝 TCP 地址的语句前，则后一个语句将不起作用。但如果将这两条语句换位位置，则允许改地址上其他协议的同时拒绝了该地址的 TCP 协议。RGNOS 支持过滤的协议如图 2 所示。

协议	描述
egrp	Cisco eigrp 路由选择协议
gre	GRE 隧道协议
icmp	internet 控制消息协议
igmp	internet 网关消息协议
ip	internet 协议
iprip	IP 隧道中 IP 协议
nos	KARQ NOS 兼容 IP 之上的 IP 隧道协议
ospf	OSPF 协议
tcp	传输控制协议
udp	用户数据包协议

图 2 RGNOS 支持协议列表

“source source-wildcard”指源地址和通配符掩码，源地址是主机或一组主机的点用十进制表示，必须与通配符掩码配合使用，用来指定源地址比较操作时必须比较匹配的位数。通配符掩码是一个 32 位二进制数，二进制“0”表示该位必须比较匹配，二进制“1”表示该位不需要比较匹配，可以忽略。例如通配符掩码 0.0.0.255，表示只比较 IP 地址中前 24 位，后 8 位 IP 地址忽略，通配符掩码 0.0.7.255 表示只比较 IP 地址中前 21 位，后 11 位 IP 地址忽略，通配符掩码 0.0.255.255 表示只比较 IP 地址中前 16 位，后 16 位 IP 地址忽略。有两个特殊的通配符掩码 0.0.0.0 和 255.255.255.255，可以用关键字“host”和“any”表示。host 表示一种精确

的匹配,使用时放在 IP 地址前,如 host 192.168.10.8 的一台主机。any 表示任何 IP 地址,在进行比较操作时不
对该 IP 地址进行比较。

这里的“operator”是指操作符,可以使用操作符“<、>、=、≠”等,具体的操作符命令如图 3 所示。

“port”指端口号,其范围是 0-65535,放在源 IP 地址后的端口号指源端口号;放在目的 IP 地址后的端口号指目的端口号。端口号 0 代表所有 TCP 端口或 UDP 端口。一些特殊的端口号可以直接用其对应的协议名称表示,如 TCP 端口号 80 可以用 WWW 表示,TCP 端口号 23 可以用 Telnet 表示,TCP 端口号 21 可以用 FTP 表示,UDP 端口号 53 可以用 Domain 表示,UDP 端口号 520 可用 RIP 表示。

目的地址和通配符掩码的结构与源地址和通配符掩码的结构相同,目的端口号的指定方法与源端口号的指定方法相同。

配置命名的访问控制列表

在较高版本的 IOS 上,都可以配置命名的访问控制列表。它的好处在于可以单独地添加或者删除列表中的一条语句,从而克服了传统的访问控制列表不能增量地更新,难于维护的弊端。

在全局模式下声明命名的访问控制列表命令如下:

```
Router (config) #ip access-list {extended|standard}
```

name

执行该命令后进入配置命名的访问控制列表语句的模式,可以逐条编写列表语句,以扩展的命名访问控制列表为例,其命令如下:

```
Router (config-ext-nacl) #perm|deny protocol  
source source-wildcard[operator port] destination  
destination-wildcard [operator port]
```

通过不断重复套用该命令即可建立起命名的访问控制列表,例如:

```
Router (config) #ip access-list extended server1  
Router (config-ext-nacl) #permit tcp any host  
192.168.10.1 eq telnet Router (config-ext-nacl)  
#permit tcp any host 192.168.10.1 eq smtp
```

```
Router (config-ext-nacl) #deny ip any any
```

```
Router (config-ext-nacl) #exit
```

```
Router (config) #int f0/0
```

```
Router (config-if) #ip access-group server1 out
```

```
Router (config-if) #exit
```

向命名的访问控制列表中添加语句与配置语句语法格式一样。若要删除一条语句,与删除大多数命令一样在该语句前加“no”,例如:

```
Router (config) #ip access-list extended server1
```

```
Router (config-ext-nacl) #no permit tcp any host  
192.168.10.1 eq telnet
```

```
Router (config-ext-nacl) #exit
```

OpenSCAP 管理主机安全

北京 曹江华

什么是 SCAP

SCAP (安全内容自动化协议)列举了各种软件产品的漏洞和各种与安全有关的软件配置问题,并提供了漏洞管理自动化的机制。SCAP 用开放性标准实现了自动化脆弱性管理、衡量和策略符合性评估。而 OpenSCAP 项目的目的则是为了提供一个开放源码的框架,从而让开源社群能够整合安全内容自动协议 (SCAP) 标准的能力。

SCAP 包含两个主要元素:一个是协议,即一组标准化格式与术语的开放规范,通过 SCAP,软件安全产品可以互通软件缺陷与安全配置信息,每一个规范也被称作一个 SCAP 组件;其次,SCAP 包括软件缺陷与安全配置标准化的参考数据,也被称作 SCAP 内容。

下面列出了目前的 SCAP 1.0 协议组件,这些组件按类型分为:列举 (Enumerations) 组,为安全与产品

相关的信息定义了标准表述符与目录；脆弱性测量与评分（Vulnerability Measurement and Scoring）组，SCAP 版本 1.0 具体包含以下六个组件（如图 1 所示）：

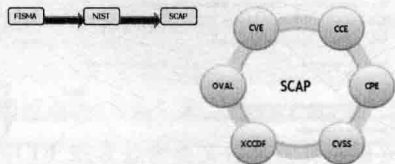


图 1 六个 SCAP 组件的示意图

OVAL（开放漏洞和评估语言）：主要是用于说明计算机的配置和发现的漏洞情况。

XCCDF（可扩展配置清单说明格式）：用于描述安全配置列表（Checklists）、基准点（Benchmarks）的相关文档。XCCDF 一般用于描述目标系统安全配置规则，是一种为表达、组织和管理安全指导的语言。

CVE（通用漏洞披露）：是包含了公众所已知信息安全的漏洞信息以及披露的集合。

CPE（通用平台枚举）：可以利用该平台列举出各项企业资产，从而为各项资产的数据提供基本的管理依据。

CCE（通用配置枚举）：其作用与 CVE 很相似，但是 CCE 主要用于处理错误配置问题。

CVSS（通用漏洞评价体系）：一种用于评估软件安全隐患的度量系统，同时它也可以以打分的方式帮助用户优先应对安全风险。

其中，在图 1 所示中，FISMA 是法规，是美国政府制定的信息安全管理法律依据。NIST 是政府授权去制定和实施标准、技术援助的机构。而 SCAP 则是 NIST 为了实施符合 FISMA 的自动化要求而制定的一个协议。

安装 OpenSCAP 软件包

使用 Yum 命令即可在线安装 OpenSCAP 相关软件包：

```
#yum install openscap-utils scap-security-guide
openscap-engine-sce scap-workbench
```

说明：“openscap-utils”是 SCAP 软件包，主要包括 Oscan 命令行工具。该工具作为一个 OpenSCAP 库的前端，基于它处理的一种类型的 SCAP 内容，将其功能分组模块化（子命令）。openscap-engine-sce 的安装包提供了脚本检查引擎（SCE）。SCE 是 SCAP 的一个扩展协议，允许内容作者使用脚本语言去编写自己的安全内容，

例如 Bash 语言，Python 语言或者 Ruby 语言。“scap-security-guide”是 SSG 软件包，它包含了 Linux 系统最新的一套安全策略。SSG 安全内容可以在“/usr/share/xml/scap/ssg/rhel7/”目录下找到。scap-workbench 是一个图形化的工具，它允许用户在本地或远程系统上执行配置和漏洞扫描，实现系统的修复，以及生成基于扫描评估的报告。

使用 Oscan 命令行工具

检查 Oscan 版本的功能：

在安装完 Oscan 后，您可以检查您所安装 Oscan 版本的功能，要显示此信息，请输入以下命令：

```
# oscan -V
```

命令输出的内容包括，系统版本（CVE、OVAL、CPE、CVSS），某个 Oscan 文件储存在什么位置，能使用什么样的 SCAP 对象，以及其他有用的信息。

扫描本地系统

Oscan 最重要的功能是在本地系统上执行配置与漏洞扫描。通常包括有两种格式：OVAL 格式以及 XCCDF 格式。

1.XCCDF 文件格式

XCCDF 语言被设计为支持信息交换、文档生成、组织化和情境化调整、自动一致性测试以及符合性评分。XCCDF 语言主要是描述性质的，并不包含任何用来执行安全扫描的命令。然而，XCCDF 文档可以作为其他 SCAP 组件的参考，而且就其本身而言，它也可以被用于制作合规策略，移植到除相关的评估文档（OVAL、OCIL）以外的所有目标平台。通常，可以用一组 XML 文件中包含一个 XCCDF 清单的方法来表示合规策略。该 XCCDF 文件通常指向了评估资源、多重 OVAL、OCIL 以及脚本检查引擎（SCE）文件。此外，该文件集可以包含有 CPE 字典文件和为此字典定义了对象的 OVAL 文件。

使用 SSG XCCDF 基准扫描系统。要在系统中为 xccdf_org.ssgproject.content_profile_rht-ccp 配置文件执行 SSG XCCDF 基准测试，请运行以下命令：

```
#oscap xccdf eval --profile rht-ccp \
--results /tmp/'hostname'-ssg-results.xml \
--report /var/www/html/'hostname'-ssg-results.html \
```



```
--cpe /usr/share/xml/scap/ssg/content/ssg-rhel7-cpe-
dictionary.xml \
/usr/share/xml/scap/ssg/content/ssg-rhel7-xccdf.xml
其中屏幕输出界面如图 2 所示。
```



图 2 屏幕输出界面

Result:图中“fail”(红色字符)表示存在安全漏洞。Result:“pass”(绿色字符)表示通过安全检查。

这份结果报告将会以“localhost.localdomain-ssg-results.html”文件为名储存在“/var/www/html/”目录下。我们可以使用浏览器打开这个检查结果文件。

2.OVAL 文件格式

OVAL(开放式漏洞评估语言)是 SCAP 中必不可少的和最初始的组成部分。有别于其他工具或者自定义脚本, OVAL 语言以声明的形式描述了资源的理想状态。OVAL 语言代码不能被直接执行, 而是依靠一个叫做扫描软件的 OVAL 解释工具去执行。OVAL 所具备的声明性质保证了受评估系统的状态不会被意外地改变, 这一点是非常重要的, 因为安全扫描工具通常运行在可能获取的最高权限上。为了评估来自 SSG 数据流文件代表的安全策略中的特别的 OVAL 定义, 请运行以下命令:

```
# oscap oval eval --id oval:ssg:def:100 --results scan-
oval-results.xml /usr/share/xml/scap/ssg/rhel7/ssg-rhel7-ds.
xml
```

OVAL 的扫描结果将会以“scan-oval-results.xml”文件格式的方式保存在当前目录中。

使用 SCAP 工作台

SCAP Workbench 是一个图形化的工具, 它允许用户在本地或远程系统上执行配置和漏洞扫描, 从而实现系统的修复, 以及生成基于扫描评估的报告。与 Oscan 命令行实用工具比起来, SCAP 工作台只具备有限的功能。SCAP 工作台也可以处理只以 XCCDF 文件和数据

流文件形式存在的安全内容。安装 SCAP Workbench 软件包后通过终端即可启动, 其工作界面如图 3 所示。

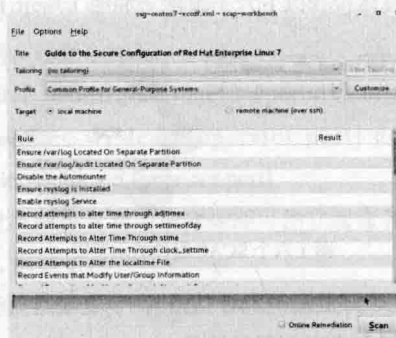


图 3 工作界面

CAP 工作台窗口包含许多交互式组件, 简单介绍一下主要组件:

Title(输入文件): 该字段包含了所选安全策略的完整路径。

Tailoring(裁剪)可以对 XCCDF 中所定义的检查单进行剪裁和调整, 该下拉列表框显示的是将被应用于所选安全策略中的清单的名称。如果存在不止一个清单, 您可以通过点击此下拉列表框来选择一个特定的清单。该下拉列表框会通知您给定安全策略的定制情况。您可以通过点击该下拉列表框来选择自定义规则, 这些规则将会被应用在系统评估中。默认值是“no tailoring”, 这意味着所使用的安全策略将不会有任何改变。如果您对所选的安全配置文件做了任何改动, 可以通过点击“Save Tailoring”按钮以 XML 文档的方式保存这些改动内容。

Profile(配置文件): 该下拉列表框包含所选安全策略配置文件的名称。通过点击该下拉列表框, 您可以从给定的 XCCDF 或者数据流文件中筛选出安全配置文件。若要创建一个继承了所选安全策略配置文件属性的新配置文件, 请点击“Customize”按钮。

Target(目标): 这两个单选按钮允许您选择待评估系统是本地计算机还是远程计算机。

Status bar(状态栏): 这是一种图形化的工具条, 指示着正在执行的操作状态。

Oline Remediation(在线修复): 该复选框允许在系统评估中开启修复功能。如果您选中该复选框, SCAP 工作台将尝试校正那些无法匹配策略定义状态的系统设置。

Scan(扫描): 该按钮允许启动对指定系统的评估。

使用 SACP 工作台扫描系统

SACP 工作台的主要功能是依照给定的 XCCDF 或者数据流文件，在被选中的系统中执行安全扫描。若要评估您的系统有没有违反所选的安全策略，请遵循下列步骤：

首先通过点击“File”和“Open Content”按钮打开相应的 XCCDF 或者数据流文件来选择一项安全策略。然后点击“Scan（扫描）”开始扫描系统，当系统扫描结束以后，新的按钮包括：“Clear”和“Save Report”以及“Show Report”，会出现并取代“Scan”按钮如图 4 所示。

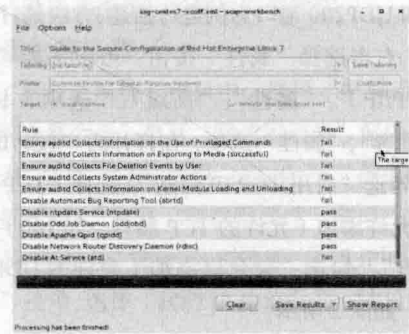


图 4 扫描系统结束后的界面

说明：

pass（绿色字符）：目标系统（及其相关组件）满足所有规则的条件 XCCDF。

fail（红色字符）：目标系统（其特定的组件）不符合某些条件的 XCCDF 规则。

除了“fail”和“pass”两个最常见的选项，还有几个选项。

error：没有能够完成规则评估。

notapplicable：规则并不适用于在此系统上进行测试（可以理解为扫描规则不匹配的）。

unknown：未知错误。

结语

本文从整体上介绍了什么是 SCAP，SCAP 的组成元素，SCAP 元素之间的关系和 SCAP 相关的开源工具，以及如何利用 SCAP 和开源工具对系统进行配置合规性扫描。可以看到使用 SCAP 能够非常方便地对系统配置合规性进行自动化评估。

❖ 关闭 Windows 系统危险端口

端口既可以用于 Windows 系统之间的网络通信，也可以作为黑客入侵的主要途径。因此端口也具有一定的安全风险。为了便于读者关闭 Windows 系统的危险端口，防止黑客入侵，本文总结了几种常见的关闭 Windows 系统端口的方法。

系统关闭法

系统关闭法，就是利用 Windows 系统图形界面的直观操作设置来关闭危险的端口。利用该方法可以关闭常见的一些端口，如 TCP23、80、135、139、445、3389 端口，

UDP137、138 端口等等，其典型的方法如下：

1.TCP23 端口

TCP23 端口主要用于为 Windows 系统提供 Telnet 服务。

其关闭方法为：依次选择“控制面板”、“管理工具”打开“服务”对话框，选择停止并禁用“Telnet”服务，如图 1 所示。

▼ 石家庄 李冲霄

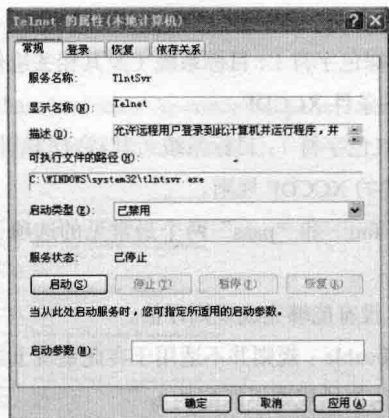


图 1 Telnet 属性

2.TCP80 端口

TCP80 端口主要用于为 Windows 系统提供 HTTP 服务。

关闭方法是：依次打开“控制面板”、“管理工具”以及“服务”对话框，选择停止并禁用“World Wide Web Publishing Service”服务选项。

3.TCP135 端口

TCP135 端口主要用于为 Windows 系统提供 RPC(远程过程调用)服务。

关闭方法是：依次选择“开始”、“运行”选项，执行命令“dcomcnfg”，然后依次选择“组件服务”、“计算机”和“属性”选项，选择“默认属性”，去掉“在此计算机上启用分布式 COM”前面的勾选项的设置即可完成。

4.UDP137、UDP138 和 TCP139 端口

UDP137 和 UDP138 端口主要用于为 Windows 系统提供计算机名称和 IP 地址的查询服务，而 TCP139 端口则主要用于为 Windows 系统提供基于 SMB 协议的文件和打印机共享服务。

这个三个端口的关闭方法是：依次选择“网上邻居”、“属性”、“本地连接”、“属性”、“TCP/IP 属性”、“高级”以及“WINS-NetBIOS 设置”选项，打开“WINS-NetBIOS 设置”对话框，选择“禁用 TCP/IP 上的 NetBIOS”选项。

5.TCP445 端口

TCP445 端口主要用于为 Windows 系统提供基于 CIFS 协议的文件和打印机共享服务。

关闭方法是：依次选择“开始”、“运行”选项，执行命令“regedit”选项，打开“注册表”窗口，在 HKEY_LOCAL_MACHINE\System\Controlset\Services\NetBT\Parameters 路径下新建名称为“SMBDeviceEnabled”，数值为“0”的 REG_DWORD 选项。

6.TCP3389 端口

TCP3389 端口主要用于为 Windows 系统提供远程桌面服务。

关闭方法是：依次选择“控制面板”、“管理工具”以及“服务”选项，停止并禁用名为“Terminal Services”的服务。

TCP/IP 筛选关闭法

TCP/IP 筛选关闭法，就是利用本地连接属性中的 TCP/IP 筛选来过滤，该方法仅允许指定端口通过，其余端口默认全部屏蔽与外界的通信，下面以只打开 TCP100 和 UDP200 端口为例进行描述，方法是：打开“本地连接”，右击选择“属性”按钮，依次选择“Internet 协议 (TCP/IP)”、“属性”、“高级”、“选项”标签页、“TCP/IP 筛选”、“属性”选项，在打开的“TCP/IP 筛选”对话框中勾选“启用 TCP/IP 筛选”，选择“TCP 端口”，勾选“只允许添加（允许的 TCP 端口，如 100）”，打开“UDP 端口”，勾选“只允许添加（允许的 UDP 端口，如 200）”，如图 2 所示。

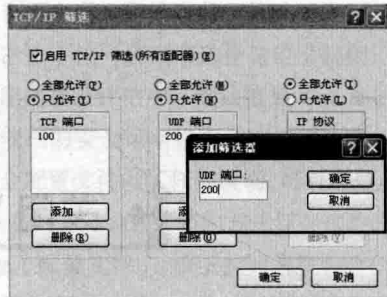


图 2 TCP/IP 筛选

IP 安全策略关闭法

IP 安全策略关闭法，就是通过 IP 安全策略来关闭 Windows 系统的端口，该方法可以关闭任意的 Windows 端口，下面以关闭 TCP4899 和 UDP135 端口为例进行描述，其关闭方法为：

1. 打开本地安全策略

依次打开“控制面板”、“管理工具”和“本地安全策略”选项，打开“本地安全策略”窗口。

2. 创建 IP 安全策略

在“本地安全策略”窗口中，右击依次选择“IP 安全策略”和“创建 IP 安全策略”选项，点击“下一步”

选项之后填写策略名称,单击“下一步”选项,去掉“激活默认响应规则”前面的勾选项,点击“下一步”以及“完成”选项,打开“新建的 IP 安全策略属性”窗口。

3. 添加 IP 安全规则

在“新建的 IP 安全策略属性”窗口中,去掉“使用‘添加向导’”前面的勾选项,添加“IP 安全规则”,打开“新规则属性”窗口。

4. 添加筛选器操作

在“新规则属性”窗口中选择“筛选器操作”选项,去掉“使用‘添加向导’”前面的勾选项的设置,选择添加“筛选器操作”的选项,打开“筛选器属性”对话框,依次打开“安全方法”标签页、“阻止”和“常规”对话框,填写好“筛选器操作”名称后完成操作。

5. 添加筛选器

在“新规则属性”窗口中,选择“IP 筛选器列表”,添加“筛选器列表”,打开“筛选器列表”窗口,填写“筛选器列表”名称,去掉“使用‘添加向导’”前面的勾选项,添加“筛选器”,打开“筛选器属性”窗口、“地址”标签页以及“源地址”选项,分别选择“任何 IP 地址”和“目标地址”选项,选择“我的 IP 地址”与“协议”标签页,选择“协议类型”为“TCP”,选择“到此端口”填写为“4899”,然后点击“确定”按钮。在“筛选器列表”窗口继续点击“添加”按钮,同理可以继续添加“UDP135 端口”,也可以添加其他需要关闭的端口,如图 3 所示。

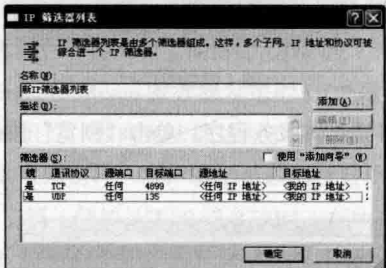


图 3 IP 筛选器列表

6. 关联并生效该规则

在“IP 安全规则属性”窗口中,选择“IP 筛选器列表”标签页,依次选择新建的“IP 筛选器列表”和“筛选器操作”标签页,选择新建的“筛选器操作”选项,然后点击“确定”按钮。最后,返回“本地安全策略”窗口中,右击新建的“IP 安全策略”,选择“指派”选项,重启计算机后,即可关闭 TCP4899 和 UDP135 端口。

防火墙关闭法

防火墙关闭法主要是利用防火墙对 Windows 系统端口进行屏蔽,该方法仅允许指定端口通过,其余端口默认全部屏蔽与外界的通信。下面以 Windows 防火墙只允许 TCP80 端口通信为例进行具体描述,方法是:依次打开“控制面板”、“Windows 防火墙”、“例外”和“添加端口”对话框,填写好名称,然后填写端口号为“80”,选择协议为“TCP”,如图 4 所示。

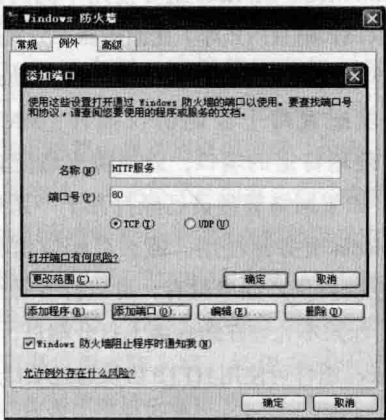


图 4 防火墙设置

经验总结

系统关闭法相对而言比较直观,操作较为简便,直接从操作系统层面对危险端口进行了关闭,但是不同端口的关闭方法各不相同,因而该方法仅适用于常见端口的关闭。TCP/IP 筛选关闭法、IP 安全策略关闭法和防火墙关闭法通用性较强,其中,TCP/IP 筛选关闭法和防火墙关闭法可以只放开任意指定的端口通信,对其他所有端口进行屏蔽,IP 安全策略关闭法则可以对任意指定的端口进行屏蔽。

但是由于这三种方法实质上是来自网络协议层对端口进行了屏蔽,让攻击者无法访问受保护的指定端口。因而建议:关闭常见端口时,使用系统关闭法;关闭不常见的端口时,使用 IP 安全策略关闭法;而如果只放开指定端口通信时,则使用 TCP/IP 筛选关闭法或防火墙关闭法。

流媒体环境下的防火墙配置

河南 倪显利

Windows Media Services 组件使用不同的协议（例如 MMS、RTSP 和 HTTP 等）在编码器、分发服务器以及客户端等之间协商连接。在 Windows Media Services 中组件可以配置每个控制协议插件（MMS、RTSP 和 HTTP）使用特定的端口，以使防火墙配置更为方便。因此，如果网络管理员已经打开了一系列端口供 Windows Media 服务器使用，那么可相应地将这些端口分配给控制协议。如果没有，可以打开每个协议的默认端口。如果不允许在防火墙上打开端口，Windows Media Services 组件可使用 HTTP 协议通过端口 80 传输。

Windows Media 服务器配置软件防火墙

Windows Media 服务器要接收和播放流媒体，首先要通过自身的软件防火墙控制，即操作系统自带“Windows 防火墙”组件的限制，因此需对其进行相关配置。以便为单播流打开默认内在使用的端口，这样要比手工打开该软件防火墙的一些有关端口要方便地多。

如果 Windows Media Services 运行在安装 Windows Server 2003 Service Pack 1 (SP1) 的计算机上，应该将 Windows Media Services 的程序（即 wmserver.exe）作为一个“例外”添加到“Windows 防火墙”中。如果 Windows Server 2003 操作系统已经加打了（SP2）补丁，将可以自动对 WMServer.exe 实现“例外”和“程序和服务”的添加过程。如果是在 Windows Server 2008 操作系统环境下，当添加“流媒体服务”的服务器角色时，可以自动实现把“Windows Media 服务”添加到“例外”的过程。确认后，下述过程可省略。

配置软件防火墙的过程在 Windows Server 2003 和 Windows Server 2008 操作系统上基本相同，这里仅以 Windows Server 2008 操作系统为例进行讨论。

1. 启动“Windows 防火墙”。依次打开“开始”、“控制面板”、“Windows 防火墙”对话框。

2. 进行“Windows 防火墙”的“更改设置”。单击“更改设置”按钮。

3. 检查“Windows 防火墙”的例外控制程序。如图 1 所示，在选项卡中单击“例外”选项，检查其中是否存在“Windows Media 服务”的项目。如果已经自动把“Windows Media 服务”添加到“例外”，以下过程可以省略。否则单击“添加程序”按钮。

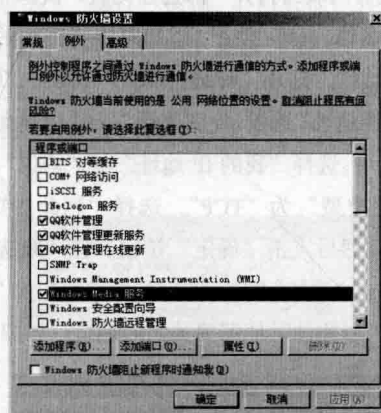


图 1 添加程序

4. 选择流媒体服务程序。单击“浏览”按钮（如图 2 所示）。

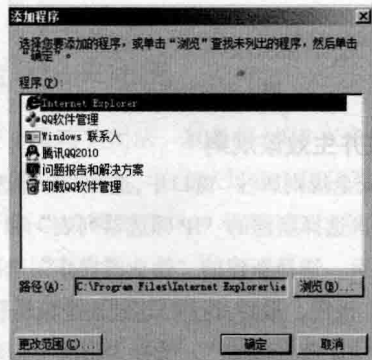


图 2 浏览

5. 选择 WMServer.exe 程序。具体为“C:\Windows\system32\Windows Media\Server\WMServer.exe”，然后

单击“打开(O)”按钮(如图3所示)。

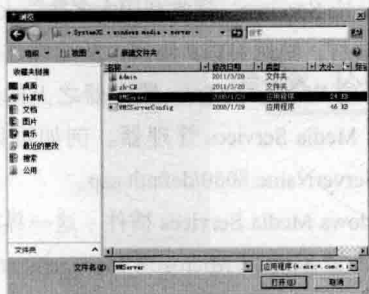


图 3 打开 WMServer.exe 程序

6. 确认添加流媒体服务程序。单击“确定”按钮。

7. 确认“Windows 防火墙设置”结果。单击“确定”按钮完成设置。

支持单播流配置防火墙

要为单播流配置防火墙,必须将服务器上启用的连接协议所需要的端口在防火墙上打开。如果要使用 MMS 或 RTSP 协议传输内容,则需同时支持 UDP 和 TCP。

要允许 Windows Media Player 和其他客户端通过 HTTP、RTSP 或 MMS 协议连接到防火墙背后的 Windows Media 服务器,为使连接 Windows Media 服务器所有版本的客户端都可以正常使用,需打开有关连接协议的相关端口,其在协议翻转过程中可能用到。

如果无法打开防火墙上的所有 UDP 的“out”端口,那么由 Windows Media 服务器发送的 UDP 数据包可能会被防火墙阻拦,因而无法抵达位于防火墙另一边的客户端处。如果是这样,客户端仍可以通过自动翻转到基于 TCP 的协议(例如:HTTP 或 RTSP)接收流。然而,翻转将导致客户端在接收流时遇到延迟。如果知道无法通过防火墙支持 UDP 流,则可以通过清除“单播数据写入器插件属性”对话框中的 UDP 复选框缩短翻转延迟。

支持多播流配置防火墙

如果使用多播流分发内容,那么网络通信将通过标准 D 类 IP 地址以及 FF00:0000:0000:0000:0000:0000:0000:0000 至 FFFF:FFFF:FFFF:FFFF:FFFF:FFFF:FFFF:FFFF 定向。第一个范围中的地址是 Internet 协议版本 4(IPv4)地址。目前这一类地址被用于多点广播(Multicast)中。第二个范围中的地址是 IPv6 地址,该版本是此协议的

新版本,它被设计用来满足快速增长地对 IP 地址的庞大需要量。并不是所有的网络都可以配置使用 IPv6 的 IP 地址,Windows Media Services 在 IPv6 的 IP 地址可以使用时将自动启用它。

Internet 不支持多播,这是因为 Internet 上的路由器不能保证全部启用多播转发机制。要进行多播,必须在网络上启用多播转发。Windows Media Services 支持的 Internet 组管理协议(IGMP)可确保只有在播放机请求多播连接的情况下才允许多播通信通过网络,因此在路由器上启用多播不会导致网络堵塞。

用在 Intranet 上时,建议使用范围 239.*.*.* 中的 IPv4 地址。端口号可以介于 1 至 65535 之间。用来传输内容的网络上的路由器必须启用多播,即路由器必须能够解释 D 类地址,否则将无法向客户端转发多播信息。

下面的防火墙配置允许多播数据包越过防火墙:

IP 多播地址范围:224.0.0.1 到 239.255.255.255。

要启用 IP 多播,必须允许发送到标准 IP 多播地址范围上的数据包越过防火墙。此 IP 多播地址范围必须同时在源服务器和播放机端以及位于其间的每个路由器上启用。

支持允许对防火墙之外的编码器进行访问

编码器使用 HTTP 连接到运行 Windows Media Services 的服务器。在默认情况下,Windows Media 编码器使用端口 8080 用于 HTTP 连接;但是编码器管理员可以指定其他的端口。如果使用其他端口,必须在指定用于 Windows Media 服务器的连接 URL 以及打开防火墙上的端口时指定同一个端口。

Windows Media 服务器可以配置成以编码器为源进行实况转播。对于一个广播发布点要进行会议实况转播编码,内容必须由编码器通过防火墙以“推传递”的方式传送到服务器,或者由服务器通过防火墙以“拉传递”的方式从编码器进行接收。

当在“推”一个数据流时,由编码器通过 8080 端口发起一个到服务器的 HTTP 连接。而另一方面,当从编码器“拉”数据流时,由服务器通过 8080 端口发起一个到编码器的 HTTP 连接。通常除编码器管理员指定一个和 8080 端口不同的端口外,是不需要配置“out”端口的。如果使用一个不同的端口,当防火墙在打开该端口后,必须在编码器连接服务器的 URL 中指定同样地端口。

如果编码器向服务器“推传递”，编码器能够成功连接 Windows Media 服务器，必须启用 Windows Media Services 管理器中的“WMS HTTP 控制协议插件”。如果服务器从编码器“拉传递”，发布点访问的路径参考 URL，例如：`http://Encoder:Port`。

下面的防火墙配置示例允许防火墙之外的运行 Windows Media 编码器的计算机通过 HTTP 访问防火墙背后的 Windows Media 服务器。“in”端口是服务器用来接受连接的端口。“out”端口是服务器用来向客户端发送数据的端口。

输入/输出：在端口 8080 上的 TCP。

支持允许分发服务器与源服务器的连接

分发服务器发布的内容来自于另一个流媒体源即源服务器，例如：另外的 Windows Media 服务器。任何运行 Windows Media Services 的计算机均可起到分发服务器的作用。源服务器是分发服务器流内容的来源，在流媒体的传输过程中分发服务器位于源服务器和客户端之间，客户端连接分发服务器就好像连接源服务器一样。

分发服务器可以放置在网络防火墙里面，流媒体源自放置在网络防火墙外面的源服务器，倘若网络防火墙里面的客户端有权访问这些内容就没有必要打开额外的端口。分发服务器可以放置在网络防火墙外面，流媒体源自放置在网络防火墙里面的源服务器，如若网络防火墙外面的客户端有权访问这些内容，同样也没有必要打开额外的端口。

支持允许管理远程服务器

通过使用下列界面管理在防火墙后面的 Windows Media 服务器：

1. 用于 Web 的 Windows Media Services 管理器：这一界面能够使管理人员很容易通过网络浏览器远程管理 Windows Media 服务器。可在窄带宽网络连接

或非 Windows 环境下使用 Web 界面越过防火墙管理 Windows Media Services。通常利用大多数防火墙没有封闭的 8080 端口，使用 HTTP 协议，从远端连接已运行 Web 服务器的 Windows Media 服务器之上的用于 Web 的 Windows Media Services 管理器。例如可以使用的 URL `http://ServerName:8080/default.asp`。

2. Windows Media Services 插件：这一界面能够使管理人员通过 MMC (Microsoft Management Console) 来管理 Windows Media 服务器，可以对运行在 Windows Server 2003 Standard Edition、Windows Server 2003 Enterprise Edition 或 Windows Server 2003 Datacenter Edition 操作系统之上的 MMC 添加插件，或者通过远程桌面连接来访问插件。

这两个管理界面需要有通过 DCOM 使用 Windows Media Services 服务的权限，为了能够访问必须为 RPC 端点映射和 DCOM 打开防火墙的 TCP 的“in”端口和 UDP 的“in/out”端口。缺省情况下，DCOM 动态为每一个应用自由选择 1025-65535 范围内其中之一需要的端口使用。为了建立高标准的安全机制，可以通过设定一个注册键为 DCOM 应用限制端口范围。

可以使用一个网络管理控制台软件，例如：Hewlett Packard 公司的 HP OpenView、Compaq 公司的 Insight Manager XE 和 Dell 公司的 OpenManage，通过 SNMP 和 WMI (Windows Management Instrumentation) 接收事件，根据这些事件可以准确快速的掌握服务器所出现的情况。为了能接收 SNMP 和 WMI 事件，必须打开防火墙的 UDP 端口 161 和 TCP 端口 445。

其他

1. 在默认情况下，使用 HTTP 传输内容是被禁用的。
2. Windows Media Services 以前被称为 Microsoft NetShow Services；一些防火墙有预先配置的 NetShow 设置，这些设置可能适用于 Windows Media Services。



内网安全防护体系的设计

湖北 刘永亮 卢永刚 喻

笔者单位信息化建设中普遍存在内网信息系统需要和外部网络实现数据交换的现实需求, 本文从系统拓扑、安全策略设计、网络 VLAN 划分及防火墙配置、服务器配置等方面提出了完整的内网信息系统安全防护体系的设计方案。

目前, 在单位的网络应用当中, 经常遇到的一类问题就是部署在单位内网上的涉密业务系统, 需要向外部网络的指定用户提供信息服务。在此类应用场景下, 如何做好内外网互联中的边界安全防护, 确保内部网络的数据和信息安全, 成为网络管理人员所面临的现实问题。笔者结合某项目的经验, 提出一种内网信息系统安全防护体系的设计方案。

安全防护体系总体设计

根据分域保护安全策略来规划设计内网整体安全防护体系, 将其整个涉密信息系统划分为多个安全域, 对每个安全域分别采用相应的安全保护措施加以保护。在满足业务、功能和地域等特性的同时, 保证整体运行的可用性、保密性和完整性的基础上, 将内网涉密系统网络划分为服务区、内部用户区等安全区域, 服务区安全域进一步划分为公共服务区、秘密级应用服务区。

整体安全防护体系由防火墙、入侵检测、网络安全审计、防病毒、补丁分发等系统设备组成。在特定应用安全域利用分别配置防火墙设置进行边界防护, 设定严格访问控制策略, 对区域间通信进行审计, 记录日志信息。通过防火墙设置统一的认证功能, 在专网中建立应用层整体的身份认证体系, 建立统一的、可控的用户管理机制, 完成对信息的安全身份鉴别式访问。入侵检测系统对访问应用服务器的连接进行深层检测。网络安全审计系统对各级安全域的访问会话进行监控, 记录访问者的操作行为。补丁分发系统及时对系统中所有漏洞进行更新和升级。

整个网络拓扑采用星形结构, 如图 1 所示。边界防火墙为网络唯一出口。防火墙采用路由模式, 将 ETH6 配置成外网接口, ETH1 接口连接病毒过滤网关。病毒过滤网关 ETH1 连接核心交换机, ETH2 连接防火墙, 病毒过滤网关采取透明桥模式连接。

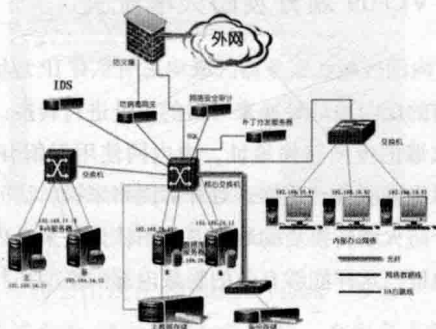


图 1 网络安全防护体系拓扑图

安全策略设计

首先, 从安全区域上, 将网络划分为: 外网区, 服务器区, 内部办公区, 并通过核心交换机对上述各个区域划分 VLAN, 以对各个区域之间的相互访问进行访问控制。并架设边界防火墙作为唯一出口, 从而实现来自外部网络的入侵的防护。

其次, 为了保护重要数据, 特将应用服务与数据服务分开, 用核心交换机进行访问控制, 保护数据的安全。

第三, 在核心交换机上部署入侵检测系统 IDS, 自动地对网络运行进行监控, 对可疑的事件给予检测和响应, 在主机和网络遭受破坏之前阻止非法的入侵行为。由于 IDS 是被动监听的特点, 所以不产生流量不会影响网络的带宽。

第四, 补丁服务器采用了 360 天擎安全管理系统解决方案, 部署一台服务器安装 360 天擎安全管理系统控制中心, 对网内终端进行统一补丁修复, 及时修复操作

系统安全漏洞,降低安全风险。

第五,在网络中部署防病毒过滤网关系统,采取与单机防护不同的基于网络的病毒防护方案。检测并记录多个网段内的病毒传输行为,在病毒侵入网络之前进行实时阻止,并且运用先进的检测技术解决了传统病毒网关类产品会造成网络延时的问题。

第六,在网络中部署网络安全审计系统,针对网络行为提供有效的行为审计、内容审计、行为报警、行为控制及相关审计功能。从管理层面提供互联网的有效监督,预防、制止数据泄密。满足用户对互联网行为审计备案及安全保护措施的要求,提供完整的上网记录,便于信息追踪、系统安全管理和风险防范。

网络 VLAN 划分及防火墙配置

对内网区域和服务器区域均采用私有 IP 地址,使用防火墙的反向地址转换来对目的地址进行转换。外网访问防火墙的反向转换地址,由内网使用保留 IP 地址的服务器提供服务。这样,对外部网络来说,访问全部是来自于防火墙转换后的地址,并不认为是来自内部网的某个地址,这样能够有效的隐藏内部网络的拓扑结构等信息。

在此次建设中,防火墙网外网接口地址配置为 27.126.242.110/25,与核心交换机口地址配置为 192.168.0.1/25,内网 VLAN 配置为 192.168.10.0/25,Web 服务器 VLAN 配置为 192.168.14.0/25,通过 IP 地址 192.168.14.15 提供网络服务,并由防火墙映射为 27.126.242.110 的公网地址。数据库服务器 VLAN 配置为 192.168.28.0/25,通过 IP 地址 192.168.28.15 提供数据服务。

同时开启防火墙的会话认证功能,为每位用户建立帐号和密码,实现只有通过认证的用户才能访问网络。具体策略为内网用户经认证通过防火墙的源地址转换功能对外网实现单向访问;外网指定用户经认证可以访问 Web 应用服务器,并对访问端口进行限制;除 Web 应用服务器(27.126.242.110)外其他所有资源外网用户均不能访问。

服务器配置

为了保证网络的高可用性与高可靠性,服务器均通

过 HA 软件实现双机热备功能,即在同一个网络节点使用两个配置相同的服务器。热备模式采用 AS 模式,即正常情况下一个处于工作状态,为主服务器,另一个处于备份状态,为备服务器。当主服务器发生意外宕机、网络故障、硬件故障等情况时,主备服务器自动切换工作状态,备服务器自动代替主服务器正常工作,从而保证了网络的正常使用。主备服务器均采用同一虚拟地址提供服务,当主服务器发生故障时,就可以透明地迁移到另一台服务器上,网络使用者不会觉察到网络链路切换的发生。

数据库服务器通过光纤直接到主存储设备。主备存储通过网络进行数据备份,备存储位于异地机房,通过光纤直连到数据库服务器所在交换机。在核心交换机上将心跳线用的网络端口和存储设备用的网络端口分别加入到不同的隔离组。

在此次实际建设中,主备 Web 服务器地址分别配置为(192.168.14.11, 192.168.14.12),主备数据库服务器地址分别配置为(192.168.28.11, 192.168.28.12)。

每两台主备服务器均采用两对心跳线作为冗余检测,应用服务器心跳线 IP 的配置为(100.100.100.10, 100.100.100.11 和 200.200.200.10, 200.200.200.11),数据库服务器心跳线 IP 的配置为(100.100.100.13, 100.100.100.14 和 200.200.200.13, 200.200.200.14)。通过 HA 软件将进行数据交互的虚拟 IP 地址切换给提供服务的服务器,再通过防火墙映射为 27.126 段的公网地址。

结语

当前绝大部分单位的业务都建立在内网信息系统的基础之上,并且需要和外网进行一定的数据交换。要保障内外网之间的信息数据和应用系统安全,并非简单的购置网络安全设备就可以解决,必须通过详细规划网络拓扑和严格设计安全策略,来构建整体安全防护体系。本文所设计的内网信息系统安全防护体系,已经在某项目中得到了成功应用,也可以为今后类似项目的建设提供参考。

巧设 Event Viewer 让 AD 更安全

威海 赵永华

Windows 系统中的 Event Viewer 是用户常用的管理工具，它可以完成许多工作，比如审核系统事件和存放系统、安全及应用程序日志等。但是 Event Viewer 还可以对活动目录 AD (Active Directory) 进行安全设置却并非众所周知，本文就透露一点 Event Viewer 在这方面的“秘技”，以博一粲。

让 AD 具有安全审计功能 (Security Auditing)

为此，需要修改当前默认的域策略，以英文版 Windows 2008 R2 为例，需要用到 Advanced Audit Policy Configuration，具体操作方式如下：

1. 依次进入“Start Menu”，“Administrative Tools”，“Group Policy Management”，然后从左侧树状结构进入“Forest”，“Domains”，并扩展开 Domain Name；
2. 右击“Default Domain Policy”，点击“Edit”，显示“Group Policy Management Editor”，依次进入“Computer Configuration”，“Windows Settings”，“Security Settings”，“Advanced Audit Policy Configuration”，“Audit Policies”，即可看到所有审计策略方面的清单，将其中的三个策略设置为支持，具体为：Domain Logon/Logoff Auditing，File System Auditing 以及 Handle Manipulation Auditing。

定制安全显示

将 AD 安全审计设为支持后，就能够接收到系统安全方面的事件信息，为此可以定制安全事件的显示 (view)，具体操作方式为：右击 Windows Logs 下的“Security”栏，选取“Create Custom View”项，选择“Critical”以及“Error”，表示在显示中只看这两类日志，

并确认在 Event logs 栏目中勾选了 Security，点击“OK”，即可显示生成显示的对话框，此时输入显示名称，比如命名为“New View”，如图 1 所示。

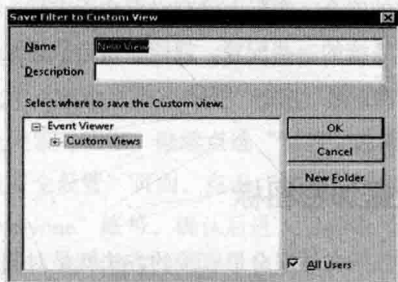


图 1 生成显示的对话框

该显示将会出现在“Custom Views”节点下，当然也可以通过点击“New Folder”生成一个保存该节点的新建文件夹，该显示提供了一个安全信息浏览窗口，其功能主要包括有三种：Import Custom View: 可以导入定制显示；Filter Current Custom View: 用于筛选重点信息；Properties: 可以改变显示名称等。

通过 Email 接收安全警报

在 Exchange Server 上可以对 Event Viewer 进行配置，将特定类型的日志通过 Email 发送给管理员，具体操作如下：

在 Event Viewer 中选择一个 event，用于接收警告信息，然后从右侧面板点击链接“Attach a Task to this Log”，就会出现向导工具“Create a Basic Task”对话框，此时需要提供一个定制名称，点击“下一步”按钮就会显示注册的 event。

点击“下一步”按钮，会显示选择执行，此时我们选择“Send an email”，然后填写邮件项目即可。

动动配置，数据存取更安全

浙江 方小明

在信息技术日益普及的今天，不管是个人用户还是单位用户，需要处理和保护的数据越来越多。为了实现目的，不少用户常常想方设法寻找外力工具来确保数据文件存取的安全。实际上没有必要舍近求远，只要动动 Windows 系统的一些配置，就能让特定数据文件的存取操作更安全。

移除数据加密图标

保护数据文件安全最直接的方法就是对其采取加密保护措施。Windows 系统中自身就有加密保护措施，除集成有新兴的 BitLocker 加密技术外，还保留了原有的 EFS 加密技术。但在使用 EFS 时，被保护的数据文件会出现明显的加锁图标，而且 NTFS 系统会以不同的颜色显示，这会很清楚地暴露目标文件。

可以采取如下操作移除数据加密图标：依次单击“开始”、“运行”命令，弹出系统运行对话框，输入“regedit”命令并回车，开启系统注册表编辑器运行状态。在该编辑界面左侧列表中，将鼠标定位到注册表节点“HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Explorer\Shell Icons”上，如图 1 所示。在目标节点选项的右侧区域，用鼠标右键单击空白位置，从弹出的右键菜单中逐一点选“新建”、“字符串值”命令，将新创建的字符串值名称设置为“178”，并鼠标双击，在对应键值对话框中，输入一个空白 ICON 图标的完整路径，单击“确定”按钮。重启计算机后，数据文件的加密图标就被成功移除了。



图 1 注册表编辑器

拒绝解密威胁数据

如果存储私密数据的系统登录密码不够“健壮”，非法用户很轻松就能借助外力暴力破解登录密码。因此建议动动组策略配置，启用相关密码策略，强制用户使用更复杂、更安全的密码来保护系统登录的安全。

首先启用帐户锁定策略，强制登录密码输入次数超过规定后自动将相关帐户锁定起来，并且在帐户锁定期满之前无法继续进入系统。在进行该操作时，先依次单击“开始”、“运行”命令，弹出系统运行对话框，输入“gpedit.msc”命令并回车，弹出系统组策略编辑界面。在该界面左侧区域，逐一跳转到“本地计算机策略”、“计算机设置”、“Windows 设置”、“安全设置”、“帐户策略”、“帐户锁定策略”分支上。双击指定分支下的“帐户锁定阈值”选项，切换到如图 2 所示的设置框，输入合适的登录尝试失败次数。正常来说，将该登录次数输入为“3”到“5”次为宜，确认后保存即可。

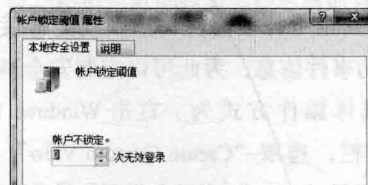


图 2 账户锁定阈值

接着强制使用更多密码位数，建议普通用户密码所

包含字符应该不少于 12 个，管理员级别的密码字符数应要达到 15 个字符。要达到该目的，只要在系统组策略编辑器窗口左侧区域，依次跳转到“本地计算机策略”、“计算机配置”、“Windows 设置”、“安全设置”、“账户策略”、“密码策略”分支上，双击指定分支下的“密码长度最小值”选项，展开对应选项属性对话框，在其中输入“12”或“15”，单击“确定”按钮。

第三，强制定期变换登录密码内容，能有效降低安全威胁程度。在系统组策略编辑器窗口左侧区域，依次选择“本地计算机策略”、“计算机配置”、“Windows 设置”、“安全设置”、“账户策略”、“密码策略”分支选项，双击其中的“密码最长使用期限”选项，在其后界面中输入合适的密码变换间隔时间。

追踪数据存取痕迹

Windows 系统自带有强大的对象审核功能，通过这项功能可全程追踪重要数据的存取痕迹，包括对重要数据文件的编辑、修改，是否创建了目录，是否运行其中的特定程序等。例如，要追踪“F:\111”目录中的数据文件存取痕迹时，可以按照下面的操作来进行：

首先进入系统的资源管理器窗口，逐一单击“工具”、“文件夹选项”命令，弹出文件夹选项设置框，选择“查看”选项卡，将对应设置页面中的“使用简单文件共享”选项取消选中，单击“确定”按钮保存。

之后打开系统运行对话框，执行“gpedit.msc”命令，开启系统组策略编辑器。在该编辑左侧列表中，依次选中“本地计算机策略”、“计算机配置”、“Windows 设置”、“安全设置”、“本地策略”、“审核策略”分支选项，找到对应分支下的“审核对象访问”选项，同时用鼠标双击，弹出如图 3 所示的对话框，勾选“成功”、“失败”等选项，确认后返回。

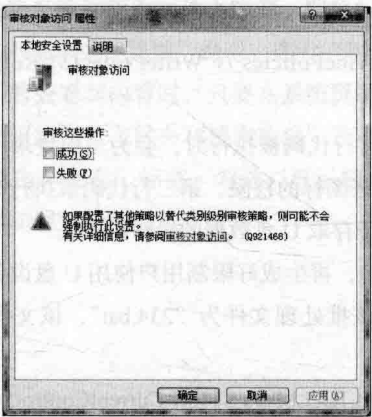


图 3 审核对象访问

接着在系统资源管理器窗口中，打开“F:\111”目录的右键菜单，单击“属性”命令，选择“安全”选项卡，在安全选项页面中点击“高级”按钮，展开特定目录的高级安全设置对话框。继续点选“审核”选项卡，切换到“高级安全设置”页面，点击“添加”按钮，选择并添加“Everyone”账号，确认后进入目标账号的审核项目列表窗口，将“遍历文件夹 / 执行文件”、“创建文件 / 写入数据”、“创建文件夹 / 附加数据”等选项的“成功”、“失败”操作都勾选（如图 4 所示）。如此“F:\111”目录的有关操作就会被 Windows 系统智能审核追踪。

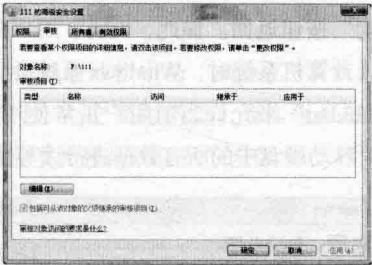


图 4 高级安全设置

智能授予数据权限

在公共场合往往会发生重要数据被通过 U 盘悄悄带走的现象。实际上，可以按需分类，为不同用户智能授予不同等级的 U 盘数据访问权限。

要实现这种控制目的时，首先通过文本编辑程序创建好用户既可以正常显示 U 盘内容，又能存取其中数据的脚本文件，假设该脚本文件的名称为“123.bat”，其中的代码内容为：

```
reg add HKLM\SYSTEM\CurrentControlSet\Services\
USBSTOR /v Start /t Reg_Dword /d 00000003 /f
```



```
reg add HKLM\SYSTEM\CurrentControlSet\Control\
StorageDevicePolicies /v WriteProtect /t Reg_Dword /d
00000000 /f
```

其中首行代码被执行时,会为当前登录用户授予显示 U 盘分区图标权限,第二行代码被执行时,会为当前用户授予存取 U 盘数据的操作权限。

同样地,再生成好限制用户使用 U 盘设备的脚本文件,假设该批处理文件为“234.bat”,该文件中的代码如下:

```
reg add HKLM\SYSTEM\CurrentControlSet\Services\
USBSTOR /v Start /t Reg_Dword /d 00000004 /f
```

上述代码执行会将 U 盘所用的 USB 接口强制定义为禁用状态,日后非法用户即使将 U 盘插入到计算机中,也不能通过它转移数据。

下面以“abc”用户账号登录进入计算机系统,逐一单击“开始”、“运行”命令,展开系统运行对话框,输入“gpedit.msc”命令,单击“确定”按钮弹出系统组策略编辑界面。在该界面的左侧显示区域中,依次选择“本地计算机策略”、“计算机配置”、“Windows 设置”、“脚本(启动/关机)”分支选项,双击指定分支下的“启动”组策略,切换到如图 5 所示的选项设置框。按下“添加”按钮,在其后界面中添加先前生成“123.bat”脚本文件,单击“确定”按钮返回。如此,“abc”用户账号日后再次登录进入计算机系统时,Windows 系统会智能执行脚本文件“123.bat”来允许当前用户正常使用移动硬盘,同时允许对移动硬盘中的所有数据进行读写操作。

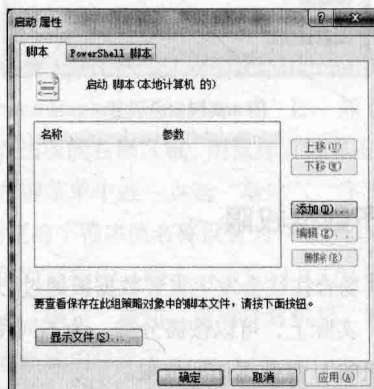


图 5 启动属性

之后以“bcd”用户账号登录进入计算机系统,按照同样的操作方法,将“234.bat”批处理文件添加到启动组策略中,这样“bcd”用户日后完成系统登录操作后,计算机将会智能调用脚本文件“234.bat”来限制用户使用计算机的 USB 接口,这时非法用户即使插入 U 盘也

无法存取其中的数据文件。

管好数据安全证书

在保护数据文件存取安全时,很多用户会首选 Windows 系统自带的 EFS 加密功能对数据执行加密操作。EFS 功能对重要数据进行加密时会产生对应的用户证书,该证书与加密的文件以及安全标识符等是相互联系的。倘若在计算机中存储了太多的加密数据和安全证书,并且要经常访问这些加密数据时,有可能会出现加密数据和安全证书在对应关系上的“混乱”问题,这将会影响到重要数据的安全存取效率。

要识别加密数据的安全证书,不妨通过查找证书的编号,直接右击特定加密文件,点选右键菜单中的“属性”命令,弹出加密文件属性设置框,选择“常规”标签,按下“高级”按钮,切换到高级设置对话框中。点击“详细信息”按钮,展开“证书缩略图”对话框,从中就能获取安全证书的唯一编号。对于其编号内容,不妨使用证书管理器来查看,逐一点击“开始”、“运行”命令,展开系统运行对话框,输入“certmgr.msc”命令并回车,进入如图 6 所示的证书管理器界面,导入安全证书,重新设置好安全证书的名称,尽量与前面获取到的证书编号对应。日后就能通过证书编号和证书文件名称的对应关系快速找到加密数据的安全证书。

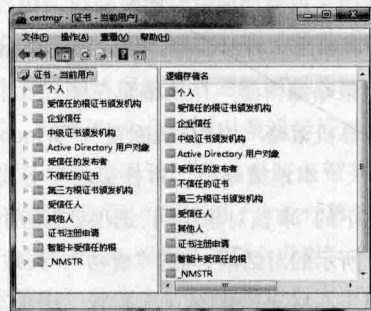


图 6 证书管理器

谨防隐私数据显现

Windows 7 以上版本系统新增有强大的数据搜索功能,用户不经意间在系统“开始”菜单的搜索文本框中输入一些关键字,或许就能将某些隐私性数据文件搜索显现出来。按如下步骤可保证隐私数据不被显现出来:首先在系统开始菜单的搜索文本框中输入“索引选项”关键字并回车,展开如图 7 所示的索引选项设置对话框;

如果系统尚未创建索引列表，则不需进行任何设置，如看到隐私数据已经出现在索引列表中，那只要按下“修改”按钮，切换到索引位置列表框，取消选中隐私数据所在的文件夹，单击确认按钮即可。

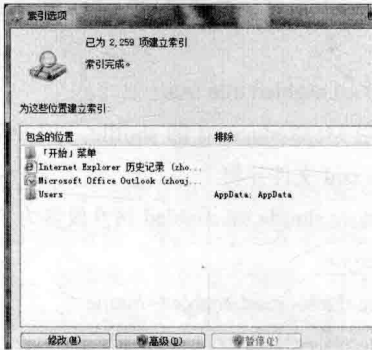


图 7 索引选项

也可将隐私数据所在文件夹隐藏，即鼠标右击特定文件夹，单击菜单中“属性”命令，选中“隐藏”选项，确认保存。若查看其内容时，只要在系统资源管理器中逐一选择“组织”、“文件夹和搜索选项”选项，在文件夹选项中单击“查看”标签，勾选“显示隐藏的文件、文件夹和驱动器”即可。

❖ Hadoop 加密静态及传输数据

▼ 山东 明红梅 长林

在真正的大数据环境中，有很多其他的数据源、数据暂存区域、临时文件和日志文件都保存着 HDFS 之外的敏感数据。当然，敏感数据在传输过程中，从终点传输到集群时，或者在企业数据从集群中的一个节点转移到另一个节点时，都必须受到保护。有一些方案可以为静态和传输的数据进行数据加密，从而使企业不仅可以满足合规要求，还可以保护信息资产的安全。

Apache Hadoop 传输加密

确保 Apache Hadoop 集群安全的首要一步是支持传输加密，这是为日后增加的每一个其他的安全层的基础。认证和 Kerberos 依赖于通信安全，所以在深入支持认证和 Kerberos 之前，必须支持数据传输的加密。

Apache Hadoop 并非是“铁板一块”的应用，正相反，它要涉及 Pig 和 Hive 直至 Impala 及 Kudu 等。这些服务可能与包括 RPC、TCP/IP 等协议在内的不同协议通信，而且每种协议都有加密数据的不同方法。使用 Web 的

都不会对浏览器地址栏中的“https://”及其旁边的锁头标志感到陌生。与之类似的是，要实现 Hadoop 中的安全通信，需要支持使用协议的安全版本。

RPC/SASL

对于与 RPC 通信的组件来说，需启用 SASL 来保护传输中的 RPC 数据。SASL 是通过在 core-site.xml 文件中设置 hadoop.rpc.protection 属性来启用，在启用此选项时有三个选项：

- 认证：提供双方间的身份验证；
 - 完整性：提供双方间的身份验证和消息的完整性；
 - 私密性：除提供认证和完整性之外，还提供机密性。
- 当然，用户可能希望选用最安全的选项，所以下面就看看在 core-site.xml 文件的内容：

```
<property>
<name>hadoop.rpc.protection</name>
<value>privacy</value>
```

```
</property>
```

改变此属性后，在集群中的所有后台程序均需重新启动，以确保所有各方都通过相同的加密协议进行通信。

TCP/IP

由于 Hadoop 的数据协议用于通过集群数据节点发送和接收数据，这种协议使用直接的 TCP/IP 套接字，并且支持通过密钥（由 RPC 进行交换）进行加密通信。为支持 TCP/IP 加密的数据流，用户需在 hdfs-site.xml 配置文件中将 dfs.encrypt.data.transfer 属性设置为“true”。这种配置的变化也必须在 NameNode 和 DataNodes 中做出改变：

```
<property>
  <name>dfs.encrypt.data.transfer</name>
  <value>true</value>
</property>
<property>
  <name>dfs.encrypt.data.transfer.algorithm</name>
  <value></value> </property>
<property>
  <name>dfs.encrypt.data.transfer.cipher.suites</name>
  <value>AES/CTR/NoPadding</value> </property>
<property>
  <name> dfs.encrypt.data.transfer.cipher.key.
bitlength</name>
  <value>256</value>
</property>
```

还可选择配置加密密码；在此案例中，已经配置了更安全的 AES-256 算法。

在改变了这种属性后，集群中的 NameNode 和 DataNode 后台程序都需要重新启动。

TLS/HTTPS

不同的 Hadoop 组件都是用不同的编码语言开发的，

例如，MapReduce 用 Java 开发，因而 SSL/TLS 可以用不同的方法进行配置。此例中检查启用 MapReduce v2 的 WebUI 的加密。

为启用 MapReduce v2 的加密 WebUI，需要编辑 core-site.xml 文件，将 hadoop.ssl.enabled 属性设置为“true”：

```
hadoop.ssl.enabled true true
```

为启用 MapReduce v2 的 shuffle，用户需要编辑 mapred-site.xml 文件并将

mapreduce.shuffle.ssl.enabled 属性设置为“true”：

```
<property>
  <name>hadoop.ssl.enabled</name>
  <value>true</value>
  <final>true</final>
</property>
```

除此之外，还有证书问题、信任存储以及其他 SSL/TLS 配置。但是，由于此文只是从一个较高的层次上进行概览而不讨论细节，而是仅仅指出用户需要从活动目录管理员或内部的 CA 获得 SSL/TLS 证书后，用正确的值来修改 ssl-server.xml 和 ssl-client.xml 文件。

HDFS 外的静态数据加密

在启用了所有 Apache Hadoop 组件中的传输数据和静态数据加密后，用户需要配置的最后一方面就是 HDFS 之外的数据加密。

虽然有些企业可能会考虑加密硬盘，但并不普遍，而且还要求专门的和更为昂贵的硬件。相反，可以利用 Linux 的本地静态数据加密特性，即 dm-crypt。

通过 dm-crypt 和 LUKS 用户可以创建一个加密的块设备，使其位于用户的标准存储设备之上，并且在其读写文件时对数据进行加密或解密。虽然由于 Cryptsetup 等工具的使用可以使建立 dm-crypt 块设备相当简单，但加密口令的存储和保护并非不重要，并且要求谨慎规划和测试。

移动设备安全使用全监控

江苏 周勇生

移动设备凭借插拔方便、操作简便等特点，受到了越来越多用户的青睐。不过，它在给数据移动存储带来方便的同时，也带来不小的安全隐患。为保护系统运行安全，有必要采取措施加强对移动设备插拔状态进行全监控，以杜绝移动设备的混乱使用。

监控染毒状态

不少病毒都能利用移动设备进行传播，如何监控在本地计算机系统中偷偷插拔过带毒的移动设备，不需要借助外力工具帮忙就能查看到插入到本地计算机中的所有移动设备以及其 ID，以下就是详细的监控操作步骤：

首先逐一点击“开始”、“运行”选项，展开“运行”对话框，打开“MS-DOS 命令行”窗口。在该窗口命令行提示符状态下，执行“reg query HKLM\SYSTEM\CurrentControlSet\Enum\USBSTOR /s”字符串命令，Windows 系统就会自动将插入到本地计算机中的所有移动设备信息列出，如图 1 所示。当然，执行“reg query HKLM\SYSTEM\CurrentControlSet\Enum\USBSTOR /s”命令后，Windows 系统有时会返回大量的结果信息，这些信息不能在一屏界面中显示完，为了可以准确查看到监控结果，不妨在 MS-DOS 工作窗口中，输入字符串命令“reg query HKLM\SYSTEM\CurrentControlSet\Enum\USBSTOR /s >H:\123.txt”，将命令返回结果输出到“H:\123.txt”文本文件中。日后，启动运行记事本程序，打开“H:\123.txt”文本文件，在该文件编辑界面中依次单击菜单栏中的“编辑”、“查找”命令，将“FriendlyName”关键字全部查找出来，同时将每个关键字后面的品牌信息逐一记录下来，这样就能将所有可疑的移动硬盘全部搜索出来。

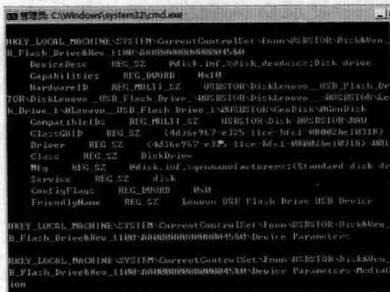


图 1 MS-DOS 命令行窗口

有时局域网中很多员工使用的移动设备都是同一品牌，这时以上方法显然行不通。由于 Windows 系统默认会为插入的每一只移动硬盘分配一个设备 ID，同时该设备 ID 是唯一的，很明显，可以利用设备 ID 来判断是否有用户在本机计算机中使用过移动硬盘。

首先将自己使用的移动硬盘插入到本地计算机中，进入“计算机”窗口，用鼠标右击移动硬盘图标，点击“属性”命令，切换到特定移动硬盘属性对话框，选择“详细信息”选项卡，在对应选项设置页面的“设备范例 ID”或“设备实例路径”设置项处，手动记下自己移动硬盘的设备 ID。

接着打开本地计算机的“开始”菜单，单击“运行”命令，弹出系统运行对话框，输入“cmd”命令并回车，切换到 DOS 命令行窗口。在该窗口命令行提示符下输入“reg query HKLM\SYSTEM\CurrentControlSet\Enum\USBSTOR /s”字符串命令，从返回的结果信息中手工记下“Disk&Ven”关键字后面的设备 ID，一旦看到结果信息中存在多个不同移动硬盘的设备 ID 时，那就表示肯定有其他用户悄悄在本机计算机中使用过移动硬盘。

监控本地状态

当在本地计算机中插拔移动设备时，Windows 系统会在后台自动监控并记忆它的状态信息。借助外力工具

USBDeview, 能轻松地读取系统监控到的内容。

开启 USBDeview 工具, 打开如图 2 所示的程序界面, 从中能看到所有移动设备的插拔记录, 包括历史的和当前的插拔信息。

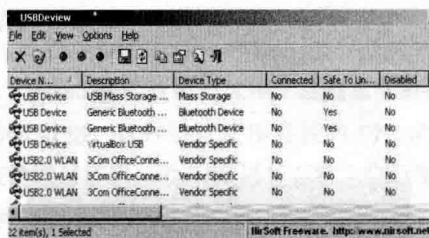


图 2 USBDeview 程序界面

对于正处于插入状态的移动设备, 如果要详细查看某个移动设备的插拔状态时, 可以从主界面的移动设备列表中, 选择目标移动设备选项, 鼠标右击打开菜单中的“Properties”命令, 切换到对应设备属性对话框, 可看到详细的插拔信息。

当然, 也可以将本地移动设备插拔状态的监控记录导出成文件, 以便日后查询。在进行该操作时, 先从设备列表界面中选择特定监控记录, 右击打开菜单“Html Report Selected Items”命令, 这样就能将选中的移动设备插拔状态导出成 HTML 格式的文件了。如果要将所有移动设备的插拔状态导出成 HTML 文件时, 只要执行快捷菜单中的“Html Report All Items”命令即可。

值得注意的是, 在特定场合下, 有时需将移动设备的插拔状态记录从计算机系统中抹除掉, 以防止用户操作隐私的外泄。只要使用电脑清理工具, 选中“USB 设备使用痕迹”选项(如图 3 所示), 再逐一按下“开始扫描”按钮和“立即清理”按钮, 可快速抹除干净移动设备的插拔状态记录。



图 3 痕迹清理

监控远程状态

在实际工作中, 常常要监控局域网其他计算机中的移动设备插拔状态, 这该如何实现呢? 使用 USB CopyNotify! 外力工具能方便地远程监控局域网中移动设备的插拔状态, 一旦发现有非法插拔现象时, 还能对其进行及时拦截。

USB CopyNotify! 工具的安装程序包包含两个部分, 一部分是客户端程序, 一部分是服务端程序。其中服务端程序主要是用来接受终端计算机移动设备的监控记录, 并生成日志文件以方便随时调用。客户端程序主要是用来监控插入到终端计算机中的移动设备状态信息, 并对可疑设备进行放行或拦截操作, 同时将监控结果反馈给服务端程序。

在本地计算机中安装 USB CopyNotify! 工具时, 必须从“Choose Components”向导对话框中选中“USB CopyNotify! Server”选项(如图 4 所示), 之后使用默认设置完成剩余安装操作。同样地, 在局域网需要被监控的普通计算机中安装 USB CopyNotify! 工具时, 一定要在“Choose Components”向导对话框中, 选中“USB CopyNotify! Client”选项, 才能保证远程监控操作获得成功。

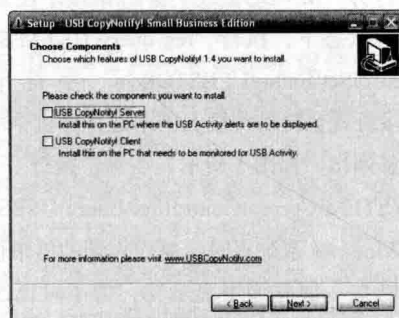


图 4 Choose Components 向导对话框

为保证远程监控的智能效果, 客户端程序在被安装成功后, 能在系统后台生成“USB CopyNotify Client Service”的服务, 以实现跟随 Windows 系统启动而自动运行目的。开启客户端程序的运行状态后, 首先进入其配置界面, 在“IP Address”位置处输入服务器端计算机的 IP 地址, 当然也可以在“Machine Name”位置处直接输入服务器端计算机的名称, 如果在这里输入“Localhost”名称(如图 5 所示), 那就意味着服务器端程序和客户端程序安装在相同的计算机中, 那么 USB CopyNotify! 工具监控的将是本地移动设备状态。在“Block USB”设置选项处, 选中“Unblock USB Drive”

选项,表示对移动设备的插拔操作进行放行,选中“Block USB Drive”选项,表示对移动设备的插拔操作进行拦截。



图 5 USB CopyNotify! Client Configuration

USB CopyNotify! 工具能够对移动设备的各种操作状态进行自动监控,其各种监控动作都会列写在“Select Alert”列表中,具体有移动设备的移除、移动设备的插入、移动设备的拦截,还有在移动设备上修改文件、更名文件、删除文件和添加文件,甚至还有关机、进入节电模式、启动结束 USB CopyNotify! 程序等。可以依照实际情况,在“Select Alert”列表中勾选合适的监控项目,同时在“Path of Execute to be Run”位置处按下“Browse”按钮,弹出“文件选择”对话框,选中并导入合适的应用程序,日后一旦 USB CopyNotify! 工具监控到移动设备的特定动作时,就能自动运行指定的应用程序,实现智能报警目的(如图 6 所示)。

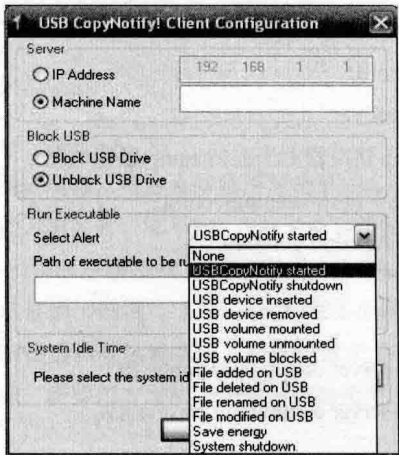


图 6 显示 Select Alert”列表设置

为了能够正确接受来自客户端程序的监控结果,还需要对服务器端程序进行合适的配置。当服务器端的 USB CopyNotify! 工具启动后,会在系统托盘区域处生成该程序的快捷图标,用鼠标右键点击该快捷图标,单击快捷菜单中的“Settings”命令,进入服务器端程序配置对话框。选中“Send Mail”选项,强制服务器端程序在接受到来自客户端的监控结果后,将监控结果发送到特定的电子信箱中。在“Mail To”位置处设置好收件人的地址,在“Mail From”位置处设置好发件人地址,在“SMTP Server”位置处输入本地邮件服务器的 IP 地址,倘若邮件服务器需要进行安全认证,不妨同时选中“Require Authentication”选项,再正确输入好登录邮件服务器的账号和密码即可。默认状态下,当服务器端程序接受到来自客户端的移动设备监控结果时,系统托盘区域处会出现相关的提示信息,如果选中了“Disable Balloon Message”功能选项,则能将报警提示功能关闭掉。如果选中“Enable Log”选项,将开启日志保存的功能,来自动存储客户端程序发送过来的移动设备监控结果,点击“浏览”按钮定义好日志文件的存储路径,如图 7 所示。

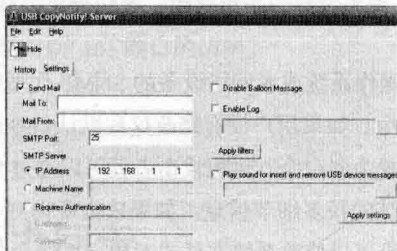


图 7 服务器端程序配置

首先选择“Apply Filters”按钮,切换到“过滤设置”对话框(如图 8 所示),在这里可以对移动设备的监控结果进行按需过滤,也包括之前介绍的所有移动设备操作类型,在不同类型的“Log”位置处,可以选择是否要对特定监控类型进行追踪记录,在“Email”位置处可以选择是否要对管理人员发送报警邮件,而在“Balloon”位置处则可以决定是否要关闭信息提示功能,在完成所有设置后,点击“Save”按钮保存。

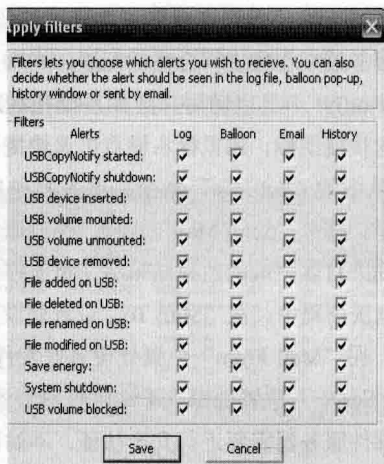


图 8 Apply filters 过滤设置

要想让监控报警效果更显著，可选中“Play Sound for Insert and Remove USB Device Messages”选项，激活“Browse”按钮，按下该功能后弹出“文件选择”对话框，导入合适的声音文件。

❖ SNMP 服务弱口令安全漏洞防范

▼ 黑龙江 丛红艺

很多操作系统或者网络设备的 SNMP 代理服务都存在默认口令。如果用户没有修改这些默认口令或者将这些口令设置为弱口令，远程攻击者就可以通过 SNMP 代理获取系统的很多细节信息。如果攻击者得到了可写口令，其甚至可以修改系统文件或者执行系统命令。

建议修改 SNMP 默认口令或者禁止 SNMP 服务，其过程为：

在 Solaris 系统下，修改“/etc/snmp/conf/snmpd.conf”中默认的口令，然后执行下列命令使之生效：

```
#/etc/init.d/init.snmpd stop
#/etc/init.d/init.snmpd start
```

在 Solaris 系统下，执行下列命令可以禁止 SNMP 服务：

```
# /etc/init.d/init.snmpd stop
# mv /etc/rc3.d/S76snmpd /etc/rc3.d/s76snmpd
```

对于像 Windows 系统，可以参考以下方法来关闭 SNMP 服务（以 Windows 2000 为例）：

打开控制面板，双击“添加或删除程序”，选择“添加/删除 Windows 组件”，选中“管理和监视工具”，双击打开，取消“简单网络管理协议”复选框，点击“确定”，

然后按照提示完成操作。

在 Cisco 路由器上可以使用如下方式来修改、删除 SNMP 口令：

1. 通过 telnet 程序或者通过串口登录进入 Cisco 路由器。

2. 进入 enable 口令：

```
Router>enable
```

```
Password:
```

```
Router#
```

3. 显示路由器上当前的 snmp 配置情况：

```
Router# show running-config
```

```
Building configuration...
```

```
...
```

```
...
```

```
snmp-server community public RO
```

```
snmp-server community private RW
```

```
....
```

```
....
```

4. 进入配置模式：

```
Router#configure terminal
```

Enter configuration commands, one per line.? End with CNTL/Z.

Router (config) #

可以选用下面三种方法中的一种或者结合使用：

1. 如果不需要通过 SNMP 进行管理，可以禁止 SNMP Agent 服务：

将所有的只读、读写口令删除后，SNMP Agent 服务就将被禁止。

a. 删除只读 (RO) 口令：

Router (config) #no snmp-server community public RO

.....

b. 删除读写 (RW) 口令：

Router (config) #no snmp-server community private

RW

.....

2. 如果用户仍需要使用 SNMP，可以选择修改 SNMP 口令，使其不易被猜测。

a. 删除原先的只读或者读写口令：

Router (config) #no snmp-server community public

RO

Router (config) #no snmp-server community private

RW

b. 设置新的只读和读写口令，口令强度应该足够，不易被猜测：

Router (config) #no snmp-server community XXXXXXXX RO

Router (config) #no snmp-server community YYYYYYYY RW

3. 只允许信任主机通过 SNMP 口令访问（以对只读口令“public”为例）。

a. 创建一个访问控制列表（假设名为 66）：

router (config) #access-list 66 deny any

b. 禁止任何人访问 public 口令：

router (config) #snmp-server community public ro 66

c. 设置允许使用 public 口令进行访问的可信主机 (1.2.3.4)：

router (config) #snmp-server host 1.2.3.4 public

对于读写口令的访问限制同上。

在对 SNMP 口令进行修改、删除等操作之后，需要执行 write memory 命令保存设置：

router (config) #exit(退出 configure 模式)

router#write memory(保存所作设置)

如果有防火墙设备，用户也可以在防火墙上过滤掉对内部网络 UDP 161 端口的访问。

❖ 让漏网病毒无力回天

▼ 江苏 孙秀洪

对付网络病毒，很多人常常简单地认为“请”出杀毒软件就能万事大吉。殊不知，现在杀毒软件能力有限，加之病毒木马程序极度狡猾，常有一些漏网病毒文件躲过杀毒软件的“围剿”。这些漏网病毒不但隐蔽性强，而且还时刻渗透和破坏着系统，对系统带来了相当大的威胁。为此，需要想方设法，让漏网病毒无力回天。

寻找漏网病毒踪迹

为了逃避杀毒软件的扫描检测，漏网病毒常常会将

自身隐藏到系统的暗角，以便让各类安全工具对其可望不可及。这时，只能手动寻找其踪迹了。

1. 从临时文件中找

在长时间工作过程中，Windows 系统会生成各式各样的临时文件，它们集中存储在系统临时文件夹中，杀毒软件对其往往无可奈何。正是基于这点，漏网病毒才会将自身混迹其中，以等待机会卷土重来。所以，及时删除各种临时文件，既能让漏网病毒无机可乘，又能有效节约宝贵的磁盘空间。

例如在 Windows 7 系统环境下，进入系统文件夹

“X:\User\用户名\AppData\Local\Temp”，可看到所有的临时文件，选中并删除，就能让所有漏网病毒全部从计算机中消失。值得注意的是，在默认状态下，“Appdata”文件夹处于不可显示状态，用户只有先打开“文件夹选项”对话框，勾选“显示所有文件和文件夹”选项，才能让该文件夹正常显示出来。

2. 从系统还原点找

为了保护数据和系统安全，有些用户会启用系统还原功能，及时为重要内容做好备份操作。而杀毒软件无法清理系统还原文件夹，这让不少漏网病毒趋之若鹜。为了对付这种类型的漏网病毒，需定期清除系统还原点，以铲除网络病毒的“温床”。

在 Windows 8 系统环境下，要删除所有的系统还原点时，可使用“Windows+X”组合键，调出系统快捷访问菜单，单击“控制面板”命令，进入系统控制面板窗口，逐一双击“系统安全”、“系统”图标，在其后界面的左侧列表区域，选择“系统保护”选项。在系统保护标签页面中，选择“配置”按钮，单击其后窗口中的“删除”按钮，可彻底删除所有的系统还原点。

3. 从引导记录中找

一些相当狡猾的漏网病毒，有时会将自身潜藏到系统的引导记录中，只要用户重新启动计算机系统，漏网病毒就会借机进入系统内存并运行。这种类型的病毒相当难缠，用户即使格式化硬盘也无法真正除掉病毒文件，毕竟其已深入到系统引导扇区中。为让此类漏网病毒无力回天，只有重新创建引导扇区记录，让病毒文件无处藏身。

使用外力工具“DiskGenius”，即可轻松对付潜藏在系统引导扇区中的漏网病毒。先使用 Windows PE 重新启动计算机系统，在 Windows PE 状态下开启目标工具的运行状态，打开对应程序主操作界面，依次单击“磁盘”、“重建主引导记录”菜单命令，确认后目标工具就会自动重新创建系统主引导记录，潜藏在引导记录中的漏网病毒文件就灰飞烟灭了。

如果不想重新创建系统主引导记录时，不妨使用更强大的安全工具——“PowerTool”，来对引导记录进行强制修复。打开目标工具的主操作窗口，逐一进入“系统修复”、“主引导记录”标签页面，按下“检测”或“强力检测”按钮，开始自动扫描测试系统引导区内容，按下“自动修复主引导记录”按钮，就能达到删除漏网病毒目的了。

4. 从系统文件中找

某些漏网病毒为了更好地躲避用户，经常会将自身伪装成系统文件，甚至直接替换掉系统文件。要想对付这类漏网病毒文件，用户只有选择去修复系统文件。

以系统管理员权限登录系统，依次单击“开始”、“运行”命令，弹出系统运行对话框，输入命令“sfc /scannow”并回车，确定后开始扫描测试所有系统文件。一旦有系统文件受到损坏时，正确放置系统安装光盘到计算机中，执行系统文件提取安装操作，就能将被漏网病毒替换掉的系统文件恢复正常。当然，如果无法成功执行“sfc /scannow”命令时，不妨尝试使用“sfc /scanonce”命令，让系统下次启动时自动扫描系统文件。

5. 从系统注册表找

有的漏网病毒会将自身拷贝到系统注册表启动项中，以实现随系统自动启动的目的。为了让这种类型漏网病毒无力回天，可以进行下面的操作来寻找并对付漏网病毒：

首先依次单击“开始”、“运行”命令，弹出运行对话框，执行“regedit”命令，打开系统注册表编辑窗口，将鼠标先定位到左侧列表中的注册表节点“HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Run”上（如图 1 所示），检查对应节点下是否存在陌生键值，如果看到陌生键值，不妨通过双击键值找出漏网病毒的源头文件，同时将其直接删除，一并删除注册表中的陌生键值。



图 1 注册表编辑器

接着将鼠标定位到注册表节点“HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Run”上，将该节点下的陌生键值所有病毒源文件依次删除。此外，还要逐一检查“HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\RunOnce”、“HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows NT\CurrentVersion\Winlogon”、“HKEY_CURRENT_USER\Software\Microsoft\

Windows\CurrentVersion\Runonce”、“HKEY_CURRENT_USER\Software\Microsoft\Windows NT\CurrentVersion\Windows”等注册表节点,看看这些节点下是否存在陌生键值,如果存在,一定要及时将陌生键值和相关病毒文件删除,这样才能将潜藏在系统注册表中的漏网病毒清除干净。

不让漏网病毒潜藏

找到并清除漏网病毒后并不意味着高枕无忧,因为其可能随时会卷土重来。还需采取一劳永逸的措施,禁止其再次潜藏到 Windows 系统中!

1. 不让潜藏到注册表中

为防止漏网病毒程序日后再次将自身拷贝到系统注册表启动项中,不妨尝试修改有关注册表节点的操作权限,具体操作为:首先依次单击“开始”、“运行”命令,输入“regedit”命令,切换到系统注册表编辑窗口,选中“HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Run”节点选项,再依次单击“编辑”、“权限”命令,弹出权限设置对话框(如图 2 所示),在这里将“everyone”帐号权限设置为“读取”,将其他权限全部设置为“拒绝”,同时将其其他普通账号删除掉,并单击“确定”按钮保存设置操作即可。同样,将其他节点的“everyone”帐号权限设置为“读取”,将普通账号权限全部设置为拒绝。

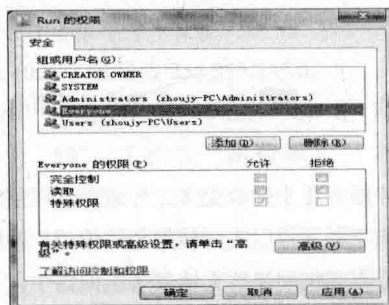


图 2 权限设置

2. 不让潜藏到组策略

有的漏网病毒隐蔽性很强,往往将自身潜藏到系统组策略中,这样普通用户甚至杀毒软件都很难发现。可以采取下面的操作方法来配置系统组策略:

首先逐一点击“开始”、“运行”命令,弹出系统运行对话框,输入“gpedit.msc”命令并回车,展开组策略编辑对话框,在该对话框的左侧显示区域,将鼠标定位到“本地用户和组”、“用户配置”、“管理模板”、“系统”、

“登录”节点上。在指定节点的右侧显示区域中,用鼠标右键单击“在用户登录时运行这些程序”选项,打开如图 3 所示的选项设置框,取消“已启用”选项的选中状态,确认后保存设置操作。

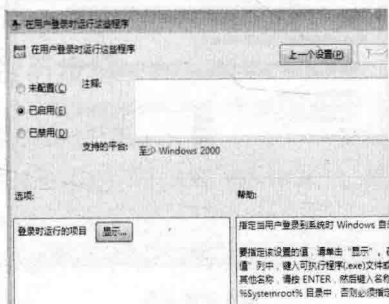


图 3 在用户登录时运行这些程序设置

3. 不让潜藏到临时目录

系统临时目录是漏网病毒程序的一个好去处,倘若事先将系统临时目录“封杀”,日后漏网病毒就不能潜藏其中了:首先逐一单击“开始”、“运行”命令,弹出系统运行对话框,输入“gpedit.msc”命令并回车,开启组策略编辑器。在该编辑界面的左侧列表中,将鼠标定位到“计算机配置”、“Windows 设置”、“安全设置”、“软件限制策略”、“其他规则”节点上。

接着选中“其他规则”选项,用鼠标右键单击该选项,从弹出的右键菜单中执行“新路径规则”命令,在其后界面“路径”位置处(如图 4 所示),输入系统临时目录路径,或直接单击“浏览”按钮,将临时目录导入进来。之后打开“安全级别”下拉列表,选择“不允许”选项,确认后漏网病毒程序就无法将自身潜藏到系统临时目录中了。

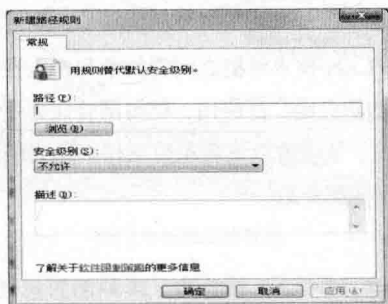


图 4 新建路径规则

4. 不让潜藏到还原点中

Windows XP 以上版本系统都支持系统还原功能,漏网病毒经常会将自身隐藏到系统还原点中。可进行如下操作关闭系统还原功能:

右击“我的电脑”或“计算机”图标,选择“属性”

命令,弹出系统属性设置对话框。点击“系统还原”选项,切换到如图 5 所示的对话框,勾选“在所有驱动器上关闭系统还原”选项,点击确认。

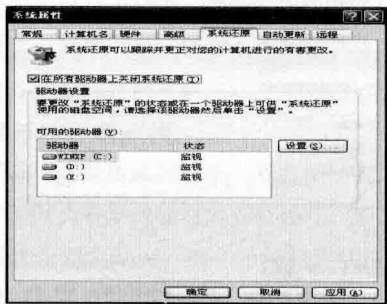


图 5 系统属性

5. 不让潜藏到主页面中

有的漏网病毒会悄悄修改 IE 浏览器主页面,同时将自身潜藏到默认主页面中去,用户一旦进入 IE 浏览器窗口,这些漏网病毒就能自动运行。可以采取如下操作进行设置:

首先在系统运行对话框中,输入“regedit”命令,开启注册表编辑器运行状态。将鼠标定位到注册表“HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\

Internet Explorer\MAIN”节点上(如图 6 所示),逐一点选“编辑”、“权限”命令,展开特定节点选项的权限设置对话框。在“组或用户名称”设置项处,将“everyone”的“读取”权限设置为“允许”,将其他权限设置为“拒绝”,并且将其他一些陌生的用户账号全部删除。

同样地,再将鼠标定位到“HKEY_CURRENT_USER\Software\Microsoft\Internet Explorer\Main”注册表节点上,打开对应节点的权限设置框,仅将“读取”权限授予“everyone”账号,删除其他陌生账号,最后重新启动本地系统。



图 6 注册表编辑器

多 VLAN 环境下防火墙配置

河北 张伟君 苗增良 陆明京

运用 VLAN 技术可提高网管效率和安全性,随着支持 VLAN 的防火墙广泛应用,使得网管能力更强,更灵活便捷。以下笔者就以笔者单位工作中防火墙跨 VLAN 管理为例做详细介绍。

需求分析

随着信息化进程的加速,单位构建了跨城区多区域信息网络(如图 1 所示)。中兴 ZXR10 T40G 为企业核心区域交换机,在各分支机构部署了可网管三层交换机。为方便管理,总部对部门及下级单位通过 VLAN 进行业务划分,取得了较好效果。但随着业务的发展,因下级

单位的业务服务逐步融合交叉,导致原有网络结构的安全控制功能不强,难以实现精细化的管控。为解决这些问题,单位将联想网御防火墙部署到网络中,方便对各区域网络业务功能进行精确控制。

网络拓扑如图 1 所示,ZXR10 T40 核心交换机划分多个 VLAN,其中 VLAN20、VLAN21 对应下级单位 1 的网段,VLAN30 对应下级单位 2 的网段,VLAN10 为本级内网段。本单位特殊通信服务(以下简称 TSTX 服务)要求网络区段间的访问规则必须满足以下规则:1. 防火墙默认策略为禁止。2.VLAN20 和 VLAN21 之间允许 TSTX 服务。3.VLAN10 对 VLAN20、VLAN21、VLAN30 允许 TSTX 服务。

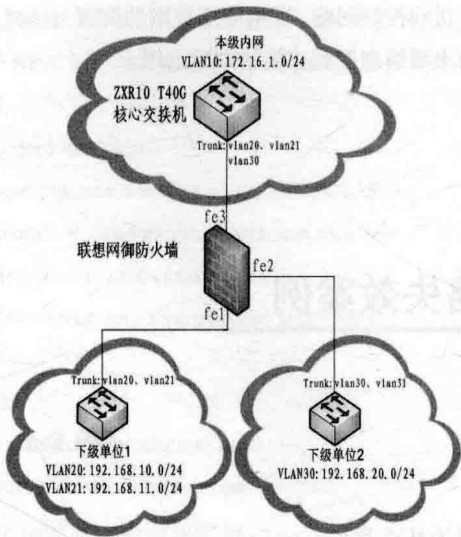


图 1 网络拓扑

配置方案

由于最初未考虑到下级单位 1 中有两个 VLAN，TSTX 服务需要跨 VLAN，所以在配置防火墙时只是添加了地址段，并对防火墙端口进行进出流控制，最终导致下级单位 1 的 VLAN20 和 VLAN21 之间不能正常使用 TSTX 服务。经过分析认为必须在防火墙中创建 VLAN 设备，并对 VLAN 设备进行策略配置，才能使下级单位 1 中的两个 VLAN 间正常使用 TSTX 服务。为此，规划以下配置方案：

- 1.Fe1 连接下级单位 1 交换机的 TRUNK 口，IP 地址为 192.168.100.1，掩码为 255.255.255.0。
2. 创建 VLAN 设备 Fe1.20，绑定设备 Fe1，VLAN ID 为“20”，工作在“路由模式”，IP 地址为 192.168.10.1，掩码为 255.255.255.0。
3. 创建 VLAN 设备 Fe1.21，绑定设备 Fe1，VLAN ID 为“21”，工作在“路由模式”，IP 地址为 192.168.11.1，掩码为 255.255.255.0，如图 2 所示。

网络配置>>接口管理>>VLAN设备

设备名称	IP地址/掩码	工作模式	绑定设备	VLAN ID	开启策略管理	是否启用	操作
Fe1.20	192.168.10.1/255.255.255.0	路由模式			×	✓	🔍 🗑
Fe1.21	192.168.11.1/255.255.255.0	路由模式			×	✓	🔍 🗑

添加 删除 停用

第1页/共1页 跳转到 1 页 60 每页 20 行

图 2 创建 VLAN 设备

- 4.FE2 连接下级单位 2 交换机的 TRUNK 口，IP 地址为 192.168.200.1，掩码为 255.255.255.0。

- 5.FE3 接到核心交换机 ZXR10 T40G，IP 地址为 172.16.1.1，掩码为 255.255.255.0。
- 6.VLAN20 网关为 192.168.10.1，VLAN21 网关为 192.168.11.1，VLAN30 网关为 192.168.20.1。

操作流程与步骤

首先添加地址资源：

- 1.VLAN20_NET 为 :192.168.10.0，掩码 为 255.255.255.0。
- 2.VLAN21_NET 为 :192.168.11.0，掩码 为 255.255.255.0。
- 3.VLAN30_NET 为 :192.168.20.0，掩码 为 255.255.255.0。
- 4.VLAN10_NET 为 :172.16.1.0，掩码 为 255.255.255.0。

其次配置访问策略：

1. 添加包过滤规则：源地址 VLAN20_NET，目的地址 VLAN21_NET，服务 TSTX，动作为允许，如图 3 所示。

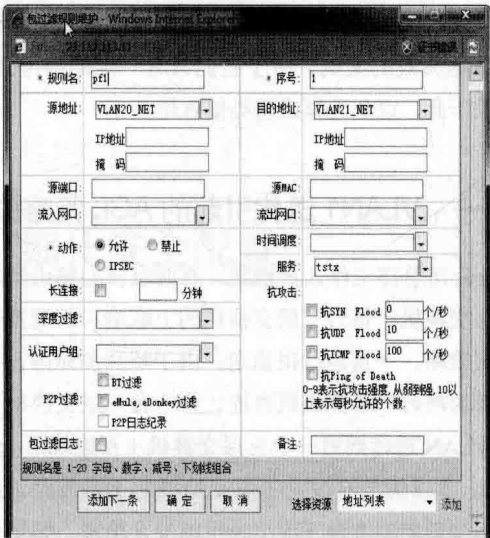


图 3 添加包过滤规则

2. 添加包过滤规则：源地址 VLAN21_NET，目的地址 VLAN20_NET，服务 TSTX，动作为允许。
3. 添加包过滤规则：源地址 VLAN10_NET，目的地址 VLAN20_NET，服务 TSTX，动作为允许。
4. 添加包过滤规则：源地址 VLAN10_NET，目的地址 VLAN21_NET，服务 TSTX，动作为允许。
5. 添加包过滤规则：源地址 VLAN10_NET，目的

地址 VLAN30_NET, 服务 TSTX, 动作为允许。

通过对防火墙内 VLAN 设备和访问规则的配置, 实现了本单位专用服务功能要求, 有效解决了跨多个

VLAN 访问控制问题。其他应用规则的配置可依此类推, 实现防火墙精准控制功能的灵活运用。

访问控制策略失效案例

安徽 叶明

近几年网络安全工作受到越来越多的重视, 由于一些公司内网的建设的不完备导致公司在网络层面上遭受着巨大安全风险。因此公司内部也加大了对安全防护工作的考核。从事安全工作的朋友都知道, 要想构建一个稳定且强健的内部网络, 除了及时给终端服务器打补丁、开防火墙之外, 对网络设备实施恰当的安全访问控制策略实在是非常重要, 因为它不仅是一种有效的技术手段, 亦是一种管理手段。

不过笔者有两次遇到过因某种特定原因, 致使访问控制策略失效的案例, 由于它们具有一定的参考意义, 特记录于此, 以免大家遭遇类似麻烦。

案例一: VLAN1 透传引起的 ACL 策略失效

分公司总部工作人员密集, 有两台核心路由器与五台三层交换机, 每台三层交换机的上联端口都配置有安全访问策略, 一直运行很稳定。由于特殊的原因, 我们将其中的两台三层交换机直连, 将一台三层交换机下的一个 VLAN 透传到另一个三层交换机 (互连线是 access 端口)。本以为没有改动三层交换机的上联线路, 这个变更不会影响到两台三层交换机的安全策略, 结果很快在省公司的例行扫描中, 发现了其中一台三层交换机下许多本已屏蔽的漏洞, 而且交换机中不停的有拓扑变更警告。

原来一般支持 802.1Q 的华为交换机在端口没有配置的时候默认都是属于 VLAN1, 也就是默认不打标签的 VLAN, 它一般不承载用户数据也不承载管理流量, 只承载控制信息。即使配置了端口为其他 VLAN 号, 这种不打标签的数据包也是默认允许通过的。所以这就不

难解释为什么我们在比较新一点的华为交换机上配置 trunk 端口时, 往往会看到 “port trunk allow-pass vlan 2 to 4094” 的配置, 因为 VLAN1 默认就是开放的。那么这对我们这个案例场景的影响就是, 这根增加的网线, 使得路由器至两个三层交换机无形多了一条通路 (经过另一个交换机的 VLAN1 透传), 而在这根网线互联的端口上是没有安全策略的, 这也就是有一台三层交换机 ACL 策略失效的原因。解决的方法很简单, 只需要将互联端口改成 trunk 口, 并且显式的定义禁止的 VLAN 号与允许的 VLAN 号:

```
interface Ethernet0/2
port link-type trunk
undo port trunk permit vlan 1
port trunk permit vlan 1013
```

案例二: DHCP 改造引起的 ACL 策略失效

分公司各个端局使用的是城域网退役下来的老设备华为 MA5200F, 在全局视图配置之下, 都有对上联端口的安全策略。由于近年来公司内部改革变动力度较大, 人员机构调整频繁, 为了减少网络维护的压力, 我们进行了 DHCP 改造。可是在新增了域、新增了地址池, 并且将此域加到上联子端口实现 DHCP 功能以后, 我们才忽然发现, 原来的 ACL 策略对这个新增的地址池失效了。

查询了许多资料后我们才找到问题的原因, 原来 MA5200F 与三层交换设备 DHCP 配置方法不同, ACL 策略生效方式也有差异。MA5200F 需要先对域指定 ucl-group, 然后针对这个 ucl-group 配置 ACL 策略, 最后再在全局启用此策略, 这样才能对域内地址池的访问流量

进行过滤。

下面给出了相关的参考例子(DHCP 安全策略部分):

```
#
ip pool hbl local
gateway xxx.xxx.xxx.xxx. 255.255.255.0
section 0 xxx.xxx.xxx.2 xxx.xxx.xxx.254
dns-server xxx.xxx.xxx.xxx
dns-server xxx.xxx.xxx.xxx secondary
#
aaa
authentication-scheme none
authentication-mode none
accounting-scheme none
accounting-mode none
domain hbl
authentication-scheme none
accounting-scheme none
ucl-group 1
ip-pool hbl
#
portvlan ethernet 22 vlan 101 1
access-type layer2-subscriber
```

```
default-domain authentication hbl
authentication-method bind
#
access-group 3000
#
acl number 3000
rule 0 net-user permit ip source xxx.xxx.0.0
0.0.255.255
rule 1 net-user deny tcp destination 1 destination-port
eq 445
rule 2 net-user deny tcp destination 1 destination-port
eq 139
.....
```

由上述两个案例我们不难总结,在实际安全工作中,我们既要尊重客观规律不断丰富自己的经验,又要防止想当然的犯经验主义的错误。同时我们还可以将平时所遇到的问题以及相应的解决方案及时与人们分享,这样可以丰富自己的经验的同时也能及时警戒其他人避免类似的错误,从而达到共同进步。只有采取审慎仔细的态度,多一点反思多一点检查,才能真正打造出一个安全的网络。

❖ 优化网络性能，细化安全配置

浙江 方小明

随着信息化建设步伐越来越快,网络与信息安全也越来越重要,更是信息化建设永恒的话题。本文以笔者单位为例,介绍单位网络与信息安全建设的基本情况与问题。

网络与信息安全建设总体现状

1. 总体架构

笔者单位在 2012 年搬迁到新办公楼后,经过几年

的网络与信息安全建设,网络与信息安全的总体架构已初步形成,网络系统在 2014 年通过信息安全等级保护测评三级测评,总体架构如图 1 所示。笔者单位的网络与信息安全系统由两台互备的 H3C S10508 三层核心交换机提供各区域间的连接。

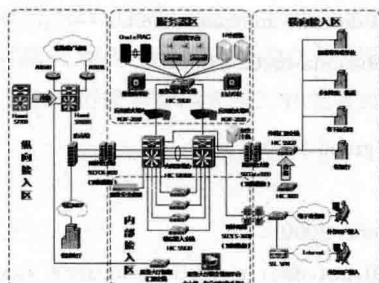


图1 总体架构图

2. 横向接入区

主要为税务分局、行政服务中心、银行、国税、乡镇街道财政所等外联单位的接入，以及各行政事业单位通过县电子政务网对县财政应用系统（如非税征管、国库集中支付系统）进行访问的业务接入。安全设备部署有2台双机模式运行的千兆防火墙，专为外联接入提供安全防护功能。部署有2台双机模式运行千兆网闸，主要为政务外网接入提供内外网安全边界隔离。

3. 纵向接入区

纵向接入区为上联至省财政厅、省地税局的连接区域，通过S6506R与AR4640、AR2831路由器经由该省市财税局至省地税局的地税广域网链路，为当前《税友龙版》、视频会议、《办税服务厅管理系统》视频监控的承载线路，该部分安全设备部署有2台双机模式运行千兆防火墙，提供省财政厅、省地税局与县局的安全边界防护功能。

4. 服务器区域

服务器区域部署了单位各种财政、地税业务的各类服务器，建有VMware vSphere 5.5虚拟化平台、Oracle数据库实时应用集群、PC服务器4余台与小型机两台，通过一台服务器汇聚交换机经两台下一代防火墙连接到核心交换机。服务器区域部署有数据库审计、安全运维管理平台、日志审计系统及堡垒机等安全设备。

5. 内部接入区

内部接入区为各楼层办公终端、视频监控接入的接入层区域，各楼层通过楼层交换机经光纤链路上联至核心交换机，内部接入终端目前部署有一套通软安全桌面准入系统。

网络与信息安全建设存在的问题

1. 财政与地税业务边界未分离

省地税局在2015年3月制定的《浙江地税系统业务专网网络边界安全防护规范》中提出：地税与财政网

络须独立部署，实现地税与财政之间终端、链路、网络与安全设备、服务器及业务应用各层级之间的相互独立运作的技术要求。按照图1所示的网络与信息安全结构图，当前为财政、地税网络混合部署，无法满足规范里规定的有：楼层终端未分离，财政地税的终端当前均使用了地税的IP地址，并未按照规范要求进行了分离；网络及安全设备未分离，财政及地税采用了同一套网络安全设备进行接入；服务器及业务应用未分离，采用了同一套网络进行接入；地税网络与财政网络的边界未分离。

2. 安全意识有待提升

随着云计算、大数据、移动互联网等一系列新技术和新应用的兴起，互联网安全形势正在发生前所未有的变化。而与此对应的却是全体干部职工相对薄弱的安全意识。而提升网络安全水平，是在提升单位安全设备的同时，更要依赖于干部职工安全意识的提升。部分干部职工对账号密码设置方式、自觉安装防病毒软件、为操作系统打补丁等一些基本的互联网安全仍不够重视，存在随意下载安装激活不熟悉的应用程序、使用非主流的应用程序、对硬盘和U盘等存储设备很少病毒查杀、随意打开不明邮件附件、轻信免费无线连接等现象。

3. 专业认证人员缺乏

在信息社会大背景下，网络与信息安全建设亟需一批既懂网络、又懂信息安全的高级信息技术人才。由于工作人员网络与信息安全意识与应用技术水平参差不齐，使网络与安全产品的选型、推广及应用产生了一定的难度，影响了网络与信息安全建设的深入和发展。网络与信息安全建设即要求全体工作人员能应用相关杀毒软件，又要求技术部门要有精通网络与信息安全的专业技术人员，这就需要我局采取切实有效的途径加大网络与信息安全全员培训力度，鼓励专业技术人员参加网络与信息安全专业化认证考试，增强财税干部网络与信息安全意识，提高信息安全实际应对能力，提升我局网络与信息安全建设队伍综合素质。

4. 网络布局受政策影响大

该单位对应到省级业务指导有省财政厅与省地税局两个业务单位，省财政厅与省地税局对网络与信息安全建设都有相关建设指导文件，如《浙江省数字财政建设领导小组办公室关于做好全省财政系统信息安全等级保护工作的通知》（浙数财办[2014]11号）、浙地税函《浙江省地方税务局关于加强地税业务专网网络边界安全防护工作的通知》（〔2015〕78号），按照文件要求，县局要对网络结构和安全设备的安全策略进行调整，牵一

发而动全身，即使是小小的调整，也要对整个的配置进行修改。

5. 终端内外网未实现物理隔离

终端物理隔离是行政事业单位防止各类黑客攻击，保护信息系统数据安全而采取的重要措施，通过终端物理隔离可以杜绝内外网络信息交换。目前该县某局部分电脑使用隔离卡形式来实现终端内外网物理隔离，但在使用过程中，内外网切换时间长，影响工作效率。

6. 安全设备的设置不够细化

如图 1，单位有安全设备 13 台，防火墙 4 台，下一代防火墙 2 台，网闸 2 台，日志审计 1 台，堡垒机、数据库审计、防毒墙与安全桌面各 1 台。安全设备设置尚不够细化，如省财政与县局之间的防火墙，目前设置为通过省财政厅能访问单位哪些服务器，但安全设置未到端口级；如在银行与 MQ 前置机服务器之间的防火墙目前设置为银行只能访问 MQ 前置机服务器，不能访问其他服务器，但设置未细化到只能访问到 MQ 前置机服务器的相应端口。

网络与信息安全建设解决方法

针对以上问题，可以从以下三大方面来解决网络与信息安全面临的相关问题。

1. 加强硬件建设，为网络与信息安全提供硬保障

为实现县局财政与地税业务边界分离，提升网络性能，强化信息安全，可以依照省地税局安全防护规范中的各项技术要求，对图 1 网络与信息安全架构进行改造，在网络与信息安全结构方面实现财政、地税的分离部署，包括核心区域分离、外联边界区域分离、业务系统分离、终端接入分离。业务边界分离后的整体架构如图 2 所示。

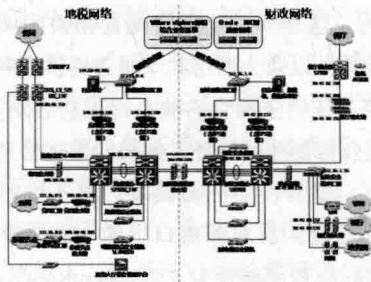


图 2 业务边界分离后的总体架构

终端内外隔离可以便于网络安全管理，避免终端外网使用过程中感染的病毒在内网广泛传播。运用虚拟桌面形式来部署外网更有利于节约成本、日常维护与信

息安全。通过小型 KVM 转换器就可实现内网计算机、虚拟桌面共用一套显示器、键盘和鼠标，节约成本开销。虚拟桌面大部分维护工作都在服务器端完成，可以极大地减少计算机维护人员维护工作量。虚拟桌面没有病毒感染的可能性，具备完美的防病毒特性，即使感染病毒也可直接删除虚拟机重新分配虚拟桌面，避免病毒传播。

2. 抓好软投入，为网络与信息安全提供理论基础

提升全局干部职工网络与信息安全意识是网络与信息安全建设的第一步，如跟局属各单位负责人签订网络与信息安全责任书，提高各单位负责人的网络安全意识；各单位指定网络信息安全管理，使网络与信息安全工作有专人负责；采用多种形式对全局干部职工定期举行网络与信息安全相关内容培训，广泛宣传网络信息安全知识，提升网络与信息安全的应对能力。

加强网络与信息安全专业人才培养是确保网络稳定与信息安全的前提。我局网络与信息安全人才缺乏，要鼓励技术人员参加计算机技术与软件专业技术资格网络与信息安全方面的考试，通过考试来加强平时的理论学习，为实际工作打下扎实的理论基础。选派技术人员参加省市局每年举行的网络与信息安全培训，提升行业内的网络与信息安全运维能力。

开展网络与信息安全检查，可以查出薄弱环节，做到防患于未然。根据相关的技术法规、标准与制度确定检查内容，再运用信息安全检测工具开展深度安全检查，确保检查取得实效。检查重点可以围绕信息安全管理、安全教育培训、技术防护、应急预案、安全问题整改等，分析安全威胁与风险，评估安全防护水平，查找突出问题和薄弱环节，确保信息安全落到实处。针对发现问题和隐患，剖析原因、明确责任、限期整改，确保实效。

3. 细化改进，为网络与信息安全提供细节支持

按照等级保护制度进行网络布局可以使网络与信息安全实施有据可依科学规范，对以后省厅省局下发的关于网络与信息安全建设文件可以很好的开展工作，而不需要大范围的调整网络结构，使网络与信息安全建设有扩展性。新建网络与信息安全系统，实施前，要实施网络与信息安全风险评估，按省厅省局的相关要求确定安全保护等级，实施过程中，进行信息安全测评，使建设的网络达到相关安全保护等级，网络投入运行后，按照网络与信息安全相关制度，定期进行信息安全检查与评估。只有在网络与信息安全实施的每个过程把关，才能网络与信息安全布局合理可靠。确保网络稳定，信息安全，为各类系统可靠运行提供保障。

优化网络配置,提升网络性能。笔者单位的网络性能的好坏很大程度上由核心交换机与楼层交换机的配置决定。优化网络配置,使用2台H3C S7506E部署IRF虚拟化,作为地税网络核心交换机,经过核心交换机虚拟化,只要通过对主交换机进行路由配置和维护,其配置和维护的信息可以同时更新到另一台交换机上,从而不需对两台交换机都进行维护,减轻维护配置工作量,提高工作效率,提升网络性能。通过对核心财政与地税核心交换机、楼层交换机配置VLAN,每个楼层财政与地税楼层交换机分别属于同一VLAN,这样很好的防止了广播风暴,并且提升了网络性能。

细化安全配置,提升防范能力。笔者单位目前防火墙安全配置大部分都基于机器级,如财政网络哪些机器可以访问地税网络中哪几台服务器,银行端哪些机器可

以访问财政端哪几台服务器,虽然这种配置可以有效防止各种非法攻击,但这种设置还不够细化,还没有到服务器的端口级,如可以把银行端哪些机器访问财政端哪几台服务器细化到银行端哪些机器可以访问财政端哪几台服务器的端口,如只开发FTP端口、MQ端口等。提高监控设备通知功能,在原只有网络机房故障通知功能的基础上,升级监控设备功能,使监控设备每天早上、晚上对机房的温度都进行通知,使机房值班人员第一时间知道机房的温度情况。开启监控设备手机卡费用最低额度通知功能,值班人员可第一时间对监控设备手机卡进行充值,避免当故障发生时监控设备手机卡因无余额而无法通知的情况发生。安全配置细化后,可进一步提升信息安全的防范能力。

驱逐病毒恢复 IE 活力

河南 刘景云

最近当笔者使用IE上网冲浪时,当打开某个网站后,IE莫名其妙的自动关闭了。当笔者再次打开IE时,发现自动进入一个内容很杂乱的站点,毫无疑问主页被恶意修改了。而且系统运行速度变得很慢,看来一定是误入了恶意网站,招来了不法程序的攻击。笔者重启电脑,发现系统运行速度变得很卡,在没有联网的情况下打开IE,之后在任务管理器中看到IE进程的高达100%,看来,一定是隐藏在IE背后病毒木马等恶意程序在捣乱。但是,运行笔者安装的某款免费杀软,对系统进行扫描检测后,却没有发现病毒的踪迹。不难看出,这要么是免费杀软不给力,要么是遇到了新型或者免杀性的病毒。没办法,只有自己动手,和病毒进行正面交锋了。

在任务管理器中仔细查看进程信息,没有发现可疑进程,看来或者是病毒隐藏了进程信息,或者是病毒没有将自身文件添加到常规启动项中。因为在没有上网的情况下,运行IE都会出现问题,病毒很可能将自身变成系统服务,或者伪装成驱动文件,来获得更高级别的运行权。运行“msconfig”程序,在系统配置实用程序

窗口中的“服务”面板中勾选“隐藏所有的Microsoft服务”项,只显示所有非系统服务。果然发现一个名为“Network Update Service”服务很可疑,因为从表面上看起来这似乎是和系统网络配置相关的服务,但实际上系统根本没有此类服务。

运行“services.msc”程序,在服务管理器中双击该服务,在起属性窗口中发现其服务名称为“wmidxsvc”,描述信息为“这是和系统网络配置相关的项目,用来设定网关参数,以及为网络共享服务提供便利,如果此服务被禁用,任何依赖它的服务将无法启动。”毫无疑问,这就是病毒创建的服务,虚假的描述信息只是在欲盖弥彰罢了。笔者决定顺藤摸瓜,将不法程序一网打尽。选中该子健,在右侧窗口中的“ImagePath”项中发现与其关联的程序路径为“%SystemRoot%\System32\wexpent32”。先在文件夹选项窗口中选择“显示所有文件和文件夹”项,同时取消“隐藏受保护的操作系统文件”项,这样可以轻松显示所有的隐藏文件。进入“C:\Windows\System32”文件夹,在其中按照创建日期

排序,让所有新文件显示在前列。因为病毒创建的文件一般日期较新,很容易查找出来。

但是,该文件并没有立即现身。笔者觉得有些奇怪,难道起彻底隐形了不成?经过按照名称顺序细致查找,才发现了该文件,原来其创建日期为2009年7月14日星期二上午7:25:06。和普通的系统文件创建日志完全相同,怪不得无法将其按照创建日期排序出来。看来,要么该文件就是系统自带的文件,要么是病毒将自身文件的创建日期进行了刻意修改,来实现鱼目混珠的目的。基于这些考虑,笔者没有冒然删除该文件。考虑到病毒也许会冒充驱动程序,从底层侵入系统,笔者决定对驱动文件进行一番检查。Windows的所有驱动文件默认都存放在“C:\Windows\System32\drivers”文件夹中,因为里面文件很多,无法准确判断其真伪。

因为系统采用的Ghost备份文件安装的,原始的Gho文件就存放在硬盘中,运行Ghost Explorer这款软件,在其主界面中点击菜单“文件”-“打开”项,选择目标Gho文件,可以显示其中包含的完整的系统文件信息,打开其中的之后打开其中的“C:\Windows\System32\drivers”,按照创建时间的顺序对两者的驱动文件信息进行比对分析,很快就发现了名为“nxwmdrv32.sys”的文件极为可疑。查看该文件的属性,发现其创建的日期为2012年12月7日。这和面提到的“wexpent32”文件的日期并不一致,主要原因笔者系统采用的是Ghost安装方式,驱动文件是由系统提供的“drive.cab”压缩解压后创建的,而“%SystemRoot%\System32”中文件是Ghost安装文件制作者在制作发布时创建的,二者之间并不完全一致。病毒入侵后,在创建非法文件时,会判断不同文件夹中原始文件的创建日期信息,然后将自身文件的创建日期进行修改,来实现混迹于其间的目的。

在注册表编辑器中点击“Ctrl+F”组合键,搜索“nxwmdrv32.sys”字符串,在“HKEY_LOCAL_MACHINE\SYSTEM\ControlSet001\Services”分支下找到了名为“nxsis32”的子键,在窗口右侧的“ImagePath”栏中发现了该文件的踪迹。根据以上信息,可以判断这是病毒伪造的驱动文件,为的是获得高级别的运行权,从系统底部侵入,这样可以有效避开杀软的监控。在“HKEY_LOCAL_MACHINE\SYSTEM\ControlSet001\Services”分支下还发现了“wmidxsvc”子键,其内容和上面提到的可疑服务完全一致。笔者将上述“nxsis32”和“wmidxsvc”删除。考虑到“nxwmdrv32.sys”和“wexpent32”文件的创建时间不一致,但是同属一个

“派系”,在驱动文件夹中是否存在和“wexpent32”文件创建日期相同的其他可疑文件呢?因为驱动文件一般都带有数字签名,于是笔者以“wexpent32”文件创建日期基准,在驱动文件夹中查找与之日期相同的文件,找到几个符合条件的文件后,逐个查看其数字签名信息。虽然病毒文件也会为找数字签名,不过难免存在马脚。经过仔细排查,果然发现名为“vrddnj.sys”的驱动文件数字签名漏洞百出,例如没有版本和公司信息等内容。在注册表编辑器中搜索“vrddnj.sys”字符串,在“KEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Services”分支下找到名为“vrddnj”的子键,在其右侧的“ImagePath”栏中显示了该文件的具体路径。看来,这也是病毒伪造驱动程序文件。

根据以上分析,将注册表中与病毒相关的键值全部删除,然后重启系统,进入安全模式,先关闭系统还原功能,因为病毒喜欢藏身到各磁盘根目录下的“System Volume Information”文件夹中,来逃避追捕。之后删除上述所有和病毒相关的文件,当删除“vrddnj.sys”文件时,系统弹出警告信息,提示该文件正在使用无法删除。运行注册表编辑器,查找和“vrddnj.sys”相关的所有项目,果然在“HKEY_LOCAL_MACHINE\SYSTEM\ControlSet001\Enum\Root\LEGACY_VRDNJ”,“HKEY_LOCAL_MACHINE\SYSTEM\ControlSet001\Enum\Root\LEGACY_VRDNJ\0000”,“HKEY_LOCAL_MACHINE\SYSTEM\ControlSet001\Enum\Root\LEGACY_VRDNJ\0000\Control”等路径中都发现了和“vrddnj.sys”相关的数据。当删除这些键值时,出现无法删除的提示,一定是病毒对其设置了禁止访问的权限所致。在对应子键的右键菜单上点击“权限”项,在弹出窗口中点击“添加”按钮,将当前账户添加进来,并赋予去完全控制的权限。之后才将其彻底删除。因为“vrddnj.sys”文件已经加载到内存中,所有无法直接删除。

为了稳妥起见,针对上述病毒文件,在注册表中又进行了一番彻底的搜索,确定没有留下什么痕迹信息。之后在开始运行中输入“%temp%”,回车后打开临时文件夹,将其中的临时文件全部删除,又启动安装的某款安全软件,清扫了所有的垃圾文件,如果有病毒残余藏身到临时文件或者缓存文件夹的话,最好将其彻底扫除。为了防止病毒在系统文件夹留有残余文件,笔者对系统文件夹进行了一番检查,果然在“C:\Windows\System32\Web”文件夹中发现了“pndxpi32.dll”,“jdsthuldrv.exe”文件,在确认是病毒文件后将去清除。在“C:\Windows\

System”文件夹中发现名为“advport.dll”的文件没有具体的开发者信息，估计和病毒存在关联，将其删除即可。

但是当笔者重启电脑进入安全模式，试图删除“vrddnj.sys”文件时，系统弹出无法删除的提示信息。在注册表编辑器中查找“vrddnj.sys”字符串，发现与其相关的项目又自动恢复了。这是为什么呢？其实道理很简单，驱动文件有很高的运行权，在系统启动会自动加载到内存中，当关机重启时内存中的驱动文件会回写到

源文件中，这样该文件就自动恢复注册表设置信息。了解这一点后，笔者在开始运行栏中执行“shutdown -t”命令，执行快速关机动作，让被病毒驱动文件无法执行回写操作。再次进入安全模式，按照上述方法成功清除了“vrddnj.sys”，并删除了其在注册表中的相关信息。之后重启系统进入正常模式，拨号上网后，IE 终于恢复正常了。

❖ 电力企业中的病毒防护

吉林 马凌巍

电力行业作为国家的经济命脉，在国民经济中具有举足轻重的作用，其网络安全问题直接关系到国家命脉。近年来，随着电力企业信息网络的建设和应用的不断发展，病毒的困扰和危害日益突出，如何构筑无毒环境、保障网络安全成为急需解决的问题，如图 1 所示。

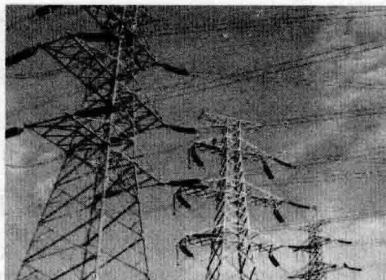


图 1 供电系统

由于电力企业的信息网络系统具有网络规模庞大，客户机及服务器数量众多，网络维护人员相对较少的特点，因此需要一套全方位、多层次、集中管理、分级维护和经济高效的病毒防护体系（如图 2 所示）。

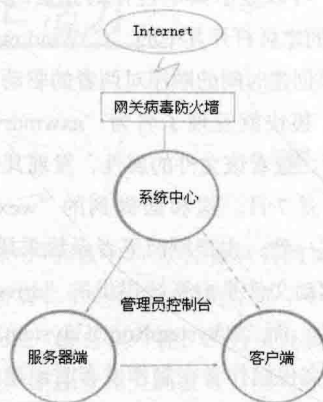


图 2 多层次病毒防护体系示意图

电力企业病毒防护系统应当考虑的几个问题

电力企业信息网络地域覆盖面广（跨越若干县、市，方圆数百平方公里），为了最大限度地防范病毒危害，在建立企业网防病毒体系时，必须针对电力企业内部网的网络构造和应用环境的实际情况，从桌面客户端、服务器、群件及网路上进行全方位、多层次的整体病毒防护。并实现整个网络防病毒策略的集中统一管理和各个网段防病毒维护工作的分级管理。

所使用的杀毒软件必须适应企业管理的需要，必须能够实现企业病毒防护策略的集中管理和分级式维护的需要。

必须对整个网络实行全方位、多层次的病毒防护，对所有可能存在的病毒的侵入点进行防护，也就是说应该在网络的每一个层次都要进行有效的病毒防护。

必须在主要服务器上实现防毒软件的远程安装，以方便企业内部的工作人员更加方便直接的完成杀毒程序的安装管理，减轻网络管理人员的工作压力。

由于现在电子邮件已成为企业应用最多的工具，因此杀毒软件必须具备最先进的邮件监控功能。当遇到感染性很强的邮件病毒时，要能够快速有效地将病毒清除，防止邮件病毒对企业造成更大的危害。

病毒定义码以及扫描病毒引擎的更新必须快速方便。

防病毒系统必须提供详细的日志，并能够分析统计病毒攻击事件的次数、原因以及来源。

多层次、分级式病毒防护体系的设计原理

针对电力企业信息网络环境的实际情况，为了保障企业信息安全和保证网络安全稳定运行，必须建立基于网络的多层次的病毒防护系统。从网络系统的各组成环节来看，多层防御的网络防毒体系应该是利用先进的分布式技术，将整个防病毒体系分为五个相互关联的子系统，分别是：系统中心、服务器端、客户端、Internet 网关和“移动式”管理员控制台。各个子系统协同工作，共同完成对整个网络的病毒防护工作，能够最大限度地完成对病毒的全面防护和查杀，如图 3 所示。

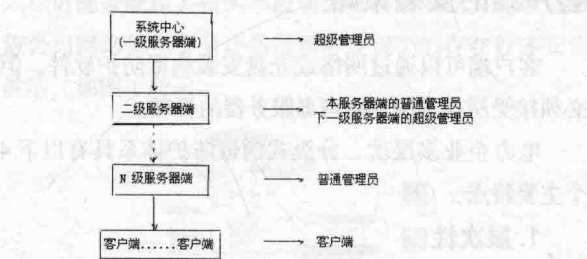


图 3 病毒防护体系集中管理、分级维护示意图

系统中心

系统中心是整个防病毒体系的信息管理和病毒防护的自动控制核心，它实时地记录防护体系内每台计算机上的病毒监控、检测和清除信息，同时根据管理员控制台的设置，实现对整个防护系统的自动控制。通过系统

中心可以实现整个信息网络防病毒策略的强制实施，以及通过其与 Internet 的实时连接获得防病毒工具的最新病毒定义代码，确保以最快的响应速度完成整个信息网络病毒防护系统自动升级。

服务器端

在各个网段设置病毒服务器，病毒服务器主要负责实时与系统中心通信，获得最新的病毒定义更新代码和最新的系统病毒防护策略。在系统中心授权后，通过服务器端可以根据本网段的实际情况定制本网段有效的病毒防护策略和定时完成在本网段的全线病毒查杀工作。系统中心通过服务器端获得各个网段的病毒监控、检测和清除信息。服务器端根据实际情况可以建立一级防病毒服务器、二级防病毒服务器等多个级别的服务器端，以便实现防病毒系统的分级管理和划地区维护。

客户端

客户端是分别针对网络应用服务器和网络工作站（客户机）设计的，承担着对当前应用服务器和工作站上病毒的实时监控、检测和清除，自动向其所属的病毒服务器报告病毒监测情况，以及自动通过病毒服务器进行升级的任务。客户端没有权利更改系统中心和所属的病毒服务器端强制布置的病毒防护策略。

Internet 网关

目前企业普遍采用的病毒防护是软件防护，即在网络接入邮件服务器、文件服务器或者工作站上进行防毒。这类软件防护因为架构在操作系统之上，所以受到了服务器的系统资源、操作系统稳定和有否漏洞的影响。因此在基于软件防毒的基础上，在电力企业信息网的 Internet 接口和广域网接口处应当配置网关级的硬件防毒墙，将网络病毒挡在“门”外，解决了软件防毒的“瓶颈”，以实现病毒防护的软硬兼施。

“移动式”管理员控制台

管理员控制台是整个防病毒系统设置、管理和控制的操作平台，它集中管理网络上所有已安装过防毒软件的计算机，同时实现对系统中心和防病毒服务器的管理，

它可以安装到任何一台安装了防毒软件的计算机上,实现“移动式”管理。管理员控制台能够直接显示每一个服务器端/客户端计算机的实时监控状态、病毒定义代码更新版本、查杀毒状态,这样管理员对于任何安装了防毒软件的计算机防毒状态都一目了然,随时对各个的防病毒情况进行监控。管理员还能够随时启动(关闭)单个(多个)服务器端(客户端计算机)上的实时监控,确保整个网络上的每台计算机都处于最佳的防护状态,同时也能保证全网随时处于高效运行之中,充分的实现了对全网的客户端和服务器的24小时不间断的查杀毒准备。

根据电力企业信息网络覆盖面积广、局客户端多,管理程序复杂的状况,电力企业病毒防护系统还应当有一个合理、有效的分级维护管理模式。有利于电力企业的统一、高效的管理。它将病毒防护的管理权限分为多个级别,在企业内部设立超级管理员和普通管理员进行分级管理。超级管理员可以创建若干普通管理员,并可任意挑选出若干客户端分派给普通管理员。而普通管理员同样也可以对自己管理的客户端进行进一步的分组,并对任意分组进行管理。在这种分级管理模式下,超级管理员和普通管理员的权限设计和职能分工是非常明确的。超级管理员具有添加删除普通管理员账号、分配计算机给普通管理员管理、对全网的计算机进行查杀毒等全面的管理职能;而普通管理员则对其网段的计算机进行分组、查杀毒等方面的管理。这种分级管理的模式使信息安全管理的工作变得更加明确和轻松。分级管理模式充分考虑到了电力企业复杂的信息网络设置,从根本上解决了电力企业网络管理难度大,操作困难这一难题,实现了对网络信息安全高效、简易的管理要求。

电力企业多层次、分级式病毒防护体系的主要布置策略具体表现在:

病毒定义代码的更新策略

如图4所示,系统中心可以和防病毒一级服务器安装在同一台服务器上,并与Internet实时相连,每天以固定时间从互联网上下载并更新最新的病毒定义代码库;二级服务器追随一级服务器下载并更新病毒定义代码库;客户端在每天的固定时间会从其所属的防病毒服务器中下载并更新病毒定义代码库,以实现网络防病毒系统的实时更新。病毒定义代码超过30天不更新就会向所属的服务器和管理员报警。

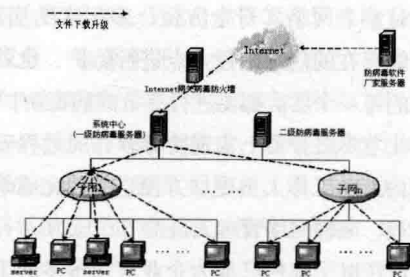


图4 病毒代码分流分级更新示意图

病毒服务器的实时防护策略

病毒服务器的实时防护策略是启动实时病毒防护功能,实时监控网络、软驱和光驱有无病毒入侵,若发现病毒,第一操作清除病毒,第二操作隔离未清除的病毒,所有的操作都记录到日志。

客户端的实时防护策略

强制启动实时病毒防护功能,实时监控网络、软驱和光驱有无病毒入侵,如果发现病毒,第一操作是清除病毒,第二操作是隔离未清除的病毒,所有的操作都记录并传送到所属的防病毒服务器端。客户端卸载防病毒软件需要密码。客户端不能停止病毒实时防护功能和操作规则。

客户端的安装策略

客户端可以通过网络或光盘安装病毒防护软件,但必须接受所在子网的防病毒服务器的管理。

电力企业多层次、分级式病毒防护体系具有以下4个主要特点:

1. 层次性

在用户桌面、服务器、Internet网关安装适当的防毒部件和硬件病毒防火墙,应当以网为本、多层次地最大限度地发挥病毒防护作用。

2. 集中性

整个信息网络的病毒防护策略是相互配合和统一制定管理的,支持远程集中式配置和管理。

3. 自动化

整个防病毒系统能自动更新病毒特征码数据库和其他相关信息。配置好后,无需人工干涉。

4. 高效性

病毒定义更新的优点在于采用分流分级管理，更新速度快，占用网络资源少，维护工作简单明了，应用和运行效率高。

5. 智能化

系统能够通过详细的日志按照预定的要求分析统计出当前网络中的病毒源及其他病毒活动情况，使网络管理员直接了解到网络中的病毒活动状况。针对一些突发问题做出快速响应。

结语

正如以上本文所论述，电力企业的信息网络系统网

络规模庞大，客户机及服务器数量众多，电力企业防毒体系的建立不能单纯地依靠几种防毒产品的堆积，它的重点在于要针对企业现有的网络环境，对网络中所有可能存在的病毒侵入点进行详细的分析，由一个或几个系统管理中心集中对企业网络进行病毒查杀，从而实现企业全网的多层次、智能化、高效性和统一性的安全管理与分级维护。

为确保网络信息的安全，企业还必须制定完善的管理制度以配合多层次、分级式病毒防护系统的有效运行。如配备相应的维护人员负责整个网络病毒防护系统的日常管理及维护；制定相应的网络病毒防护的管理制度；强制实施统一的防病毒策略等。确保网络病毒防护系统真正的为电力企业的发展保驾护航。

◆ Intranet 网络架构安全评估

▼ 湖北 杨楚华

在企业信息化建设过程中，网络是任何信息化建设的基础。企业领导、技术管理人员都必须进一步提高计算机网络安全意识，确保网络的安全、稳定运行。

某大型企业一直重视网络基础建设，并通过加大投入尽可能采取相关技术手段确保其网络安全，但通过对该公司网络架构安全评估过程中发现仍然存在较多安全缺陷，如图 1 所示。

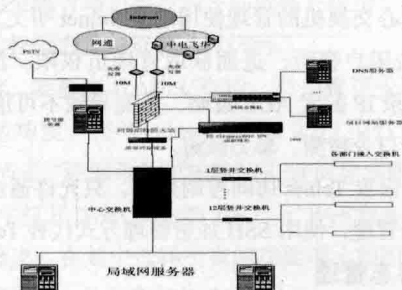


图 1 网络拓扑图

Intranet 网络架构安全评估方案

根据该公司组织结构和网络系统的特点，采取以顾问访谈、文档分析等方式，辅助安全漏洞扫描、人工安全检查等技术手段，对网络系统各方面的安全状况进行全面考察、充分分析后得到当前网络架构的现状以及评估方案。

从安全区域的角度来看，该公司整个网络架构可分为：出口区、DMZ 区、内部服务器区以及用户接入区。

对该公司网络架构评估从网络建设规范性、网络可靠性、网络边界安全性、网络协议安全分析、网络流量分析、网络通信安全、网络安全管理等 7 个方面进行全面评估，对存在的安全风险给出了下列相关建议。

网络建设规范性

1.IP 地址规划

IP 地址规划合理，地址分配易于管理，具有连续性。

2. 网络设备命名

网络设备命名不够规范。

建议采用以下命名方法：AA_xYYYY_zz。其中：AA 表示物理位置的全拼；x 表示交换机 s 或路由器 r；YYYY 表示设备型号；zz 表示设备序号，用 01、02 等表示。

3. 网络架构

网络架构清晰，层次分明，边界明确。安全边界明确，对敏感系统例如 DMZ、财务人事系统同其他系统以防火墙或者划分 VLAN 的方式进行了有效隔离。VPN 用户从外网登录后可以访问整个内网，存在一定的安全隐患。

建议严格限制 VPN 网段对内网的访问。遵循“缺省关闭，按需求开通”原则，严格限制 VPN 网段对内网的访问。

网络可靠性

1. 链路可靠性

网通与中电飞华两条互联网链路相互独立，没有充分利用做到链路互备。

建议在防火墙上进行路由设置，实现双链路互备，提高链路可靠性。

2. 设备可靠性

核心交换机和防火墙无备份，存在单点故障隐患。

建议增加一台核心交换机和一台防火墙与现网交换机和防火墙组成双机热备的工作模式，增强设备可靠性。

网络边界安全性

1. 防火墙

防火墙配置了严格的访问控制策略，有效保证了内网和 DMZ 区服务器的安全性。但对互联网开放了 radmin、telnet 等远程管理服务，存在较大的安全隐患。

建议在防火墙上配置禁止互联网用户访问 ramdin、telnet 等服务，或者配置只允许可信 IP 访问。

2. 内网 VLAN 划分

核心交换机进行了 VLAN 划分，并配置了访问控制列表(ACL)。ACL 目前只对财务和人事网段进行了保护，对于客户端访问服务器区没有任何限制措施，部分对外网提供服务的服务器与其他内网服务器在同一 VLAN，存在较大的安全隐患，如渗透测试所示，外网攻击者若控制一台外网服务器，就有可能控制整个内网。

建议根据业务需要，配置 ACL，严格限制客户端对

服务器区的访问；为对外网提供服务的服务器单独划分一个 VLAN，并在该 VLAN 与内网之间部署防火墙，严格限制内外网服务器之间的访问。

网络协议安全分析

路由协议：采用高效的静态路由协议和 OSPF 等动态路由协议相结合，对于目前的网络结构是合理有效的。

网络流量分析

流量监控、流量分析：部署了 QQview 对网络中的流量与用户行为进行监测和管理，优化了网络流量。

网络通信安全

1. 入侵检测

没有部署入侵检测设备，在本次的渗透测试过程中，即使测试人员从互联网成功进入了内网，也没有系统对以上攻击行为进行告警。

建议在互联网出口及核心交换机上部署 IDS 或 IPS，监控及阻断来自互联网及内部恶意用户的入侵行为。

2. 抗拒绝服务

未充分考虑分布式拒绝服务攻击(DDoS)的威胁，缺乏防御日益猖獗的 DDoS 攻击的有效手段。

建议部署专用的抗拒绝服务设备以增强网络安全性。

网络安全管理

1. 远程管理

对核心交换机的管理使用的是 Telnet 明文方式，容易被非法用户窃听、进而获取管理员权限。没有针对 Telnet 登录 IP 配置 ACL 策略，可能导致不可信的 IP 对设备进行口令猜测、暴力破解。

建议设置 Telnet 访问控制列表，只允许通过信任 IP 进行远程管理，使用 SSH 加密管理方式代替 Telnet。

2. 日志管理

缺乏集中日志分析系统，对设备的访问、常见信息以及异常信息的原始记录，是处理和分析问题的一个重要辅助手段和监控方式。

建议部署集中日志分析系统，协助网络管理员全面分析网络设备产生的日志。



强化 IIS 8.0 安全性

河南 郭振江

IIS 信息服务器在网络上应用的很广泛,很多网站都是基于其管理和发布的,正因为如此,IIS 服务器也成了黑客重点攻击的目标。因此,提高 IIS 服务器的安全性,是保证网站安全运行的基本条件。对于 Windows Server 2012 中提供的 IIS 8.0 来说,其拥有多层次的安全体系结构。例如,但客户端访问 Web 网站时,客户端将访问请求发送给服务器,服务器将处理结果发送回客户端,完成客户端和服务器的交互过程。实际上,对于该过程,从安全控制角度来看,可以划分为不同的层级。

例如,从 IP 层面来说,可以设置是否允许客户端访问 Web 网站。当某客户端在规定的时间内连续访问服务器,就会被服务器视为可疑用户,通过将其放置到黑名单中,该用户就无法继续访问服务器。从 HTTP 以及 HTTPS 层面来说,IIS 就可以通过设置特定的 HTTP/HTTPS 协议的特性,对用户的访问进行管控。例如,可以限制用户使用 Get, Post, Put 等方式提交数据,来有效保护服务器安全。从 IIS 层面来说,可以设置相关的身份验证协议,来检测客户端是否是合法的用户。从业务程序层面来说,同样可以限制用户的访问权限。例如当用户访问网站上的开设的论坛时,就会按照身份的不同,被划分到管理员预设的不同的账户组中,用户只能在规定的权限内,对资源进行访问。

当然,要提高 IIS 的安全性,必须保证安装好启用了对应的功能。在 Windows Server 2012 中打开服务器管理器,点击“添加角色和功能”项,在向导界面中的“角色”列表中打开“Web 服务器(IIS)”→“Web 服务器”→“安全性”分支,在其中选择所有的功能项(如图 1 所示)。点击安装按钮,执行安装操作。



图 1 添加必要的功能项目

打开 IIS 管理器,在其中可以针对服务器级别或者具体的网站,执行所需的安全设置。例如,选择某个网站,从 IP 层面设置其安全属性的话,在窗口中部双击“IP 地址和域限制”项,在右侧点击“编辑功能设置”链接,在弹出窗口中可以看到,在默认情况下,没有指定的限制条件的客户端都是可以访问该网站的。点击“添加拒绝条目”链接,在弹出窗口中可以设置特定的 IP 地址或者地址段。这样,这些 IP 客户端将无法访问服务器。

点击“编辑动态限制设置”链接,在弹出窗口中选择“基于并发请求数量拒绝 IP 地址”项,在其下可以设置并发连接的数量。当客户端在特定的时间内并发访问次数超过该值后,IIS 就会视为恶意的请求并对其进行拦截,选择“基于一段时间内的请求数量拒绝 IP 地址”项,在其下可以设置特定的时间段以及最大的请求数量。如果客户端违法了该设置,同样会被 IIS 视为恶意请求。

从 HTTP/HTTPS 层面来说,可以在窗口中部的“IIS”栏中双击“请求筛选”项,在“文件扩展名”面板右侧点击“拒绝文件扩展名”链接,在弹出窗口中输入特定的扩展名(例如“.asa”),这样当客户端试图在浏览器地址栏访问该类型的文件(例如“http://www.xxx.com/form/1.asa”等),IIS 就会返回“HTTP 错误 404.7-Not Found”之类的错误信息,拒绝用户访问这类文件。

在网站结构中,存在各种目录和文件。当不希望用户查看和访问某些目录和文件时,可以在“隐藏段”面板右侧点击“添加隐藏段”连接,输入对应的文件和目

录名称, 就可以实现上述目的。对于黑客来说, 经常使用 SQL 注入的方式, 对 SQL 数据库进行攻击。其原理是利用 SQL Server 数据库的一些漏洞, 通过构造和提交特定的 URL 地址, 来注入相关的信息, 对数据库进行渗透。为此, 可以在“URL”面板右侧点击“拒绝序列”项, 在其中窗口中输入对应的 URL, 例如“/Default.aspx?jobid=1'or'1='1”等。这样, 当黑客提交这样的 URL 时, 就会遭到 IIS 的拦截。当然, 也可以添加特定的目录和文件路径 (例如“/admin/index.asp”), 当用户试图访问这些受限制的路径时, 服务器就会返回“HTTP 错误 404.5-Not Found”之类的警告信息。

在“HTTP 谓词”面板中点击“拒绝谓词”链接, 在弹出窗口中输入对应的谓词 (例如“Post”), 这样, 当用户在对应页面中输入所需内容, 点击“提交”按钮后, 服务器就会返回“HTTP 错误 404.6-Not Found”之类的警告信息。当用户访问目标网站时, 在发送的数据包中存在一些标头信息, 例如“Host”, “ACCEPT”, “CONTENT-TYPE”, “SET-COOKIE”等。在对应标头后面跟随对应的数据信息, 例如在“Content-Length”标头后面跟随数据包内容的长度等。如果黑客使用专用工具拦截了数据包内容, 并对其标头信息进行了修改 (例如写入超长数据), 之后将该数据包发送给服务器, 就很容易造成服务器发生溢出问题, 给黑客入侵带来了可乘之机。

在“标头”面板右侧点击“添加标头”链接, 在弹出窗口中的“标头”栏中输入具体的标头名 (例如“Host”), 在“大小限制”栏中输入其数据的大小 (例如“9”)。这样, 如果用户提交的数据包中“Host”标头的长度超过该值, 服务器就会返回“HTTP 错误 404.10-Not Found”之类的错误信息。在网站中可以设置查询栏, 允许用户查询所需的内容。为了防止用户输入提交非法数据, 可以对其进行必要的限制。在“查询字符串”面板右侧点击“拒绝查询字符串”链接, 在弹出窗口中需要拒绝的内容。这样, 当用户在网站页面中查询限制的内容时, 服务器就会返回“HTTP 错误 404.18-Not Found”之类的错误。

实际上, 在“规则”面板中, 可以对各种限制条件进行集成处理。在右侧点击“添加筛选规则”链接, 在弹出窗口中输入规则名称, 选择“扫描 url”和“扫描查询字符串”项, 在“扫描标头”, “文件扩展名”以及“字符串”栏中输入对应的内容, 针对的特定的标头, 允许访问特定的文件扩展名, 拒绝访问特定的字符串。除了

使用请求筛选保护 HTTP/HTTPS 访问之外, 还可以使用授权规则来强化安全性。在“IIS”栏中双击“授权规则”项, 可以看到存在默认的授权规则。点击右侧的“编辑”链接, 可以查看其属性, 了解到其允许所有的用户进行访问。

当然, 可以添加所需的拒绝访问规则。点击右侧的“添加拒绝访问”项, 在弹出窗口 (如图 2 所示) 中可以选择限制的用户类型, 包括所有用户, 所有匿名用户, 指定的角色或者用户组, 指定的用户等。例如当使用了基本身份验证模式后, 当用户访问网站时, 就需要输入账户名和密码, 通过认证后, 才可以浏览网站。例如, 当需要对用户“fwyongh”进行控制, 可以选择“指定的用户”项, 输入“fwyongh”, 选择“将此规则应用于特定谓词”项, 输入“Get”谓词。这样当该用户在网页中查询内容, 执行提交操作时, 服务器就会返回“HTTP 错误 401.2-Unauthenticated”之类的错误信息, 说明该用户的访问收到了服务器的限制。同请求筛选相比, 授权规则可以将系统账户和 HTTP/HTTPS 特定的谓词进行关联, 让指定的用户只能访问允许的谓词, 来使用 HTTP/HTTPS 协议中相应的属性。使用授权规则和请求筛选, 可以在 HTTP/HTTPS 层面有力的保护 IIS 服务器的安全。



图 2 添加拒绝访问项目

使用相关的身份验证协议, 可以从 IIS 层面上提高安全性。在“IIS”栏中双击“身份验证”项, 可以看到提供了各种身份验证模式 (如图 3 所示)。启用的匿名身份验证方式, 允许所有用户访问 Web 服务器。

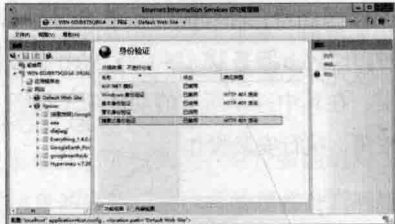


图 3 用户身份验证模式窗口

当然, 您可以根据需要对其进行控制。例如点击右

侧的“编辑”按钮,可以看到与其对应的是名为“IUSR”账户。点击“设置”,可以将其更改为别的用户。以“IUSR”账户为例,打开网站根目录中的属性窗口,在“安全”面板中点击“编辑”按钮,在“组或用户名”列表中选择“IIS_IUSRS”账户,在权限列表中的“拒绝”列中选择读取和执行,列出文件夹内容,读取等项目。保存配置信息后,当以匿名方式访问网站时,服务器就会返回“HTTP 错误 401.3-Unauthorized”的错误提示。

对于 ASP.NET 模拟方式来说,会使用 IIS 应用程序池使用的标识信息进行验证。使用 Windows 身份验证,会将访问者的账户名和密码提交给 IIS 服务器,并将其密码进行加密处理。之后服务器会验证该账户身份合法性,如果验证通过,就可以访问服务器,这适用于内部的或者加入域的客户端。对于基本身份验证来说,当用户访问时,需要输入对应的账户名和密码,这些内容会

以 Base64 方式进行加密,之后将其提交给服务器。不过这种加密方式安全性很低,为了安全起见,需要将其和 SSL 加密结合起来使用,其适用于未加入域或者外部的客户端。

对于摘要式身份验证,其支持 HTTP 1.0 协议,该模式将用户提交的凭据进行 MD5 加密,之后将其哈希值提交给 IIS 服务器,通过验证后,可以访问网站。适用于域环境,IIS 服务器必须使活动目录域的成员服务器或者域控制器,用户账户必须使活动目录域账户,并且该账户必须和 IIS 服务器位于相同的或者信任的域。选择所需的身份验证协议,点击“启用”,可以激活该验证方式。当激活多个身份验证协议,其使用是由顺序的。一般匿名身份验证方式优先级最高,之后依次为 Windows 验证方式,摘要式验证方式,基本身份验证方式。

❖ 终端账号安全不容忽视

▼ 江苏 周春生

伴随着信息化技术的日益发展,网络已成为很多单位赖以生存的重要资源,不过,越来越多的网络安全风险却成为单位面临的重大难题。尽管有不少安全风险来自外网环境,但有资料表明,在所有安全事件中,由终端账号引起的内网安全事件,所占比例正逐步上升。很显然,为了保障单位内网安全,我们需要高度重视终端系统的账号使用安全。现在,本文就从终端系统着手,总结几则安全使用账号的技巧!

监控账号创建安全

要是终端系统接入到局域网或 Internet 网络中时,那么网络中一些恶意程序可能会通过网络连接,在终端系统中偷偷创建非法用户账号,日后它们就会利用该非法账号控制或监控终端系统的运行状态了。为了保护终端计算机系统的运行安全,我们可以加大监控力度,自动监控用户账号的创建状态,日后如果有陌生用户账号

私下创建时,管理员可以在第一时间发现。

以 Windows 7 系统为例,在监控账号创建安全时,依次单击“开始”、“运行”命令,展开系统运行对话框,输入“secpol.msc”命令,开启系统安全策略编辑器运行状态。将鼠标定位于左侧列表中的“本地策略”分支上,再选中指定下的“审核策略”、“审核账户管理”选项,通过双击鼠标方式打开选项设置框,选中“成功”、“失败”选项,单击“确定”按钮保存设置操作。

接着用鼠标右键单击 Windows 系统桌面上的“计算机”图标,选择快捷菜单中的“管理”命令,展开计算机管理窗口,依次展开“系统工具”、“本地用户和组”、“用户”选项,同时用鼠标右击“用户”选项,并执行快捷菜单中的“新建用户”命令,打开新建用户对话框,在其中任意创建一个用户帐号。

之后进入 Windows 系统的控制面板窗口,逐一展开“管理工具”、“事件查看器”,切换到 Win7 系统事件查看器窗口,逐一跳转到该窗口左侧显示区域中的

“Windows 日志”、“安全”分支上,随后在“安全”分支下找到先前任意生成的用户帐号。用鼠标右键单击这个用户账号,单击快捷菜单中的“将任务附加到此事件”命令,这个时候系统屏幕上会展开附加任务向导设置对话框,依照向导提示,逐一做好报警方式、报警内容,再按“完成”按钮即可。日后,即使网络中的恶意程序悄悄在终端计算机系统中创建了非法用户账号,系统屏幕上会立即出现报警信息,根据具体的提示内容,就能识别出当前时刻是否有非法用户账号创建了。

强制账号密码安全

大家知道,现在很多终端系统由于默认存在许多安全漏洞,它遭遇病毒、木马攻击的可能性十分大,而病毒木马又会通过网络登录方式进行传播、扩散,所以限制终端系统随意通过网络进行登录或共享,是保护终端系统安全的重要途径之一。

要做到这一点,首先要强制用户账号必须使用复杂密码。只要依次单击“开始”、“运行”命令,弹出系统运行对话框,输入“gpedit.msc”命令,开启系统组策略编辑器运行状态。逐一跳转到编辑器左侧区域中的“本地计算机策略”、“计算机配置”、“Windows 设置”、“安全设置”、“账户策略”、“密码策略”节点上,双击指定节点下的“密码长度最小值”选项,展开密码长度最小值设置对话框,输入“8”或更大的数值,单击“确定”按钮后,用户账号密码最小位数将不能低于 8 个字符。

接着要让账号密码不断变化,以防别人轻易猜中。将鼠标定位到“本地计算机策略”、“计算机配置”、“Windows 设置”、“安全设置”、“账户策略”、“密码策略”节点上,双击指定节点下的“密码最长使用期限”组策略选项,打开组策略属性框,输入定期变换密码内容的间隔时间,例如输入“30”,单击“确定”按钮后退出设置对话框。这样,终端计算机系统日后会每隔 30 天就提示用户更改密码内容。

第三强制使用账号锁定功能。如果账号密码设置得不够复杂时,非法用户很可能会通过暴力破解方式,“猜”出登录密码而进行恶意操作,这样就会存在相当大的安全风险。那如何来防止非法用户猜解或者爆破远程连接密码呢?很简单!可以强制启用账号锁定功能。在系统组策略编辑窗口左侧区域,将鼠标定位到“本地计算机策略”、“计算机设置”、“Windows 设置”、“安全设置”、“账户策略”、“账户锁定策略”节点上,双击指定节点

下的“账户锁定阈值”组策略,在其后对话框中设置好触发用户账号被锁定的登录尝试失败次数,该数值范围在 0 到 999 之间,默认为“0”,也就是说,系统默认不限制登录次数。管理员可以依照工作实际,输入账户锁定次数,日后输入错误密码次数超过规定后,对应用户账号就会被强行锁定起来。

保障账号盗用安全

在进行远程网络连接的时候,恶意用户有时会通过 Windows 系统缺省的 Administrator 账号和 Guest 账号,对重要终端系统进行登录测试,要是登录测试成功,将会继续通过不同形式来非法提权,以窃取重要终端系统的所有操作权限。为了保障账号盗用安全,建议大家将缺省的用户账号名称调整为其他名称,以防止它们被非法用户轻松盗用。

例如,要调整“Administrator”账号的用户账号名称时,可以逐一单击“开始”、“运行”命令,展开系统运行文本框,在其中执行“secpol.msc”命令,进入系统安全组策略控制台窗口。在左侧显示窗格中,逐一跳转到“安全设置”、“本地策略”、“安全选项”节点上,找到指定节点下的“帐户:重命名系统管理员帐户”选项,同时用鼠标双击之,弹出组策略选项设置框,在这里输入其他复杂一些的账号名,比方说输入“Saiwojia”,再单击“确定”按钮保存设置即可。

除了“Administrator”账号会被盗用外,“Guest”账号也容易被盗用,因为该账号尽管操作权限不高,但它多数时候处于启用状态,被非法利用的机率很高,例如,恶意用户可以将该账号添加到管理员组,来进行以后的提权攻击,所以通过修改该账号名称就能预防类似攻击。在进行改名操作时,先进入终端系统安全组策略控制台窗口,将鼠标定位到“安全设置”、“本地策略”、“安全选项”分支上,双击指定分支下的“帐户:重命名来宾帐户”选项,在其后界面中设置好新的名称,确认后保存设置即可。

严控账号权限安全

一些非法用户常常会通过系统漏洞,偷偷与特定终端系统建立远程连接,再借助一些技术措施窃取系统管理员权限,打开远程桌面窗口,对特定系统进行非法操作。为了避免这种不安全现象,可以严格限制用户账号

的远程桌面使用权限，仅允许特定的管理员账号才能进行远程桌面连接，其他用户账号无权享受远程桌面权限。因为远程桌面窗口打开操作与“explorer.exe”程序访问权限有关，如果只将该程序的读取权限授权特定用户账号，就能实现上述控制目的。

在进行该操作时，先进入系统资源管理器窗口，选中“C:\Windows”目录下的“explorer.exe”程序，打开它的右键菜单，点选“属性”命令，选择属性对话框中的“安全”选项卡，删除对应选项页面中的所有用户账号。按下“添加”按钮，切换到账号选择对话框，导入可信用户账号，将其“运行”、“读取”权限修改为“允许”，单击“确定”按钮退出设置对话框。上面的设置操作，仅对没有运行的“explorer.exe”程序有效，如果该程序已经被调入内存时，那必须通过微软自行开发的“Process Explorer”工具来设置。打开该工具主操作界面，点选其中的“explorer.exe”程序，从该程序右键菜单中选择“Properties”命令，之后进入“Security”面板，单击“Permissions”按钮，在这里就能将“explorer.exe”程序访问权限，授予合法、可信用户账号了。这样，日后只有合法可信用户账号才能够拥有远程桌面权限，其他账号即使已创建好远程桌面连接，也不能打开桌面窗口进行非法攻击。

为了防止一些终端账号从低版本系统中，随意远程登录重要主机系统，建议为它们赋予带网络验证的远程桌面权限，这能避免低版本系统中的病毒感染给高版本系统。例如，在 Win7 系统中进行该操作时，可以右击 Windows 系统桌面上的“计算机”图标，点选右键菜单中的“属性”命令，进入系统属性对话框，单击“远程设置”按钮，展开远程设置界面，勾选“只允许运行带网络级身份验证的远程桌面的计算机连接”选项，单击“确定”按钮保存设置即可。

此外，要是允许空白密码用户账号随意登录终端系统，也容易给非法用户带来入侵机会。为了保护终端系统安全，建议在重要终端系统中，仅能授予空白密码用户账号控制台登录权限，不能授予其他操作权限：依次单击“开始”、“运行”命令，在弹出的系统运行对话框中，输入“gpedit.msc”命令，开启系统组策略编辑器运行状态。将鼠标定位到“本地计算机策略”、“计算机配置”、“Windows 设置”、“安全设置”、“本地策略”、“安全选项”分支上，找到指定分支下的“账户：使用空白密码的本地账号只允许进行控制台登录”选项，通过双击鼠标方式，切换到如图 1 所示的选项设置对话框。勾选“已启用”

选项，单击“确定”按钮退出设置对话框即可。

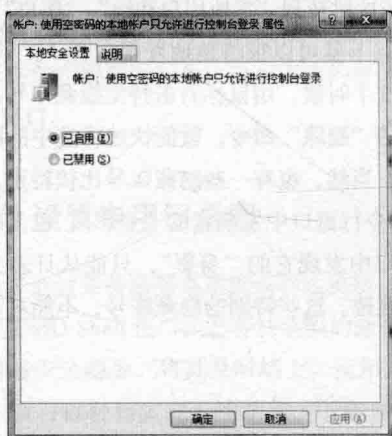


图 1 选项设置对话框

管理隐藏账号安全

一些黑客、木马擅长使用的攻击方法，就是悄悄在终端系统创建隐藏账号，并通过它进行各种非法操作，该方法有很强的隐蔽性，可以躲避杀毒软件之类的专业工具来查杀。为此，我们必须加强对系统隐藏账号的管理，确保隐藏账号的使用安全！

普通的隐藏账号，往往会在账号名后面添加“\$”后缀，来达到账号隐藏目的，黑客、木马创建好隐藏账号后，可能会悄悄将其提升为系统管理员权限，保证能通过该账号进行各种非法操作。如果想删除陌生隐藏账号，可以依次单击“开始”、“运行”命令，弹出系统运行对话框，输入“cmd”命令，在 DOS 命令行窗口的命令提示符下，执行“net localgroup administrators”命令，将所有具有系统管理员权限的隐藏账号统统显示出来。比方说，在如图 2 所示的结果界面中，我们找到一个用户名为“aaaa\$”的隐藏账号，要将其从系统中删除时，可以在 DOS 命令行窗口下输入“net user aaaa\$ /delete”命令即可。



图 2 结果界面

要是 DOS 命令不太熟悉,也可以进入计算机管理窗口,依次跳转到“本地用户和组”、“用户”节点上,在指定节点下就可以很清楚地发现包含“\$”后缀的隐藏账号。这个时候,用鼠标右击特定隐藏账号,点选右键菜单中的“删除”命令,就能快速将选中的隐藏账号删除掉了。当然,也有一些隐藏账号比较特别,既无法从 DOS 命令行窗口中发现它的“身影”,也无法从计算机管理窗口中发现它的“身影”,只能从日志文件中找到它们的痕迹。这些特别的隐藏账号,不能对它们直接

执行删除操作,只能在 DOS 工作窗口中输入“net user aaaa\$ 9876”之类的命令,调整它们的账号密码,让其无法继续生效。

还有一些隐藏账号,会躲藏在系统注册表中,要将它们删除掉时,可以先打开系统注册表编辑窗口,从中找到“HKEY_LOCAL_MACHINE\SAM\SAM\Domains\Account\Users\Names”注册表分支,在指定分支下可能会看到其他一些隐藏账号。用鼠标右键单击特定隐藏账号,从弹出的右键菜单中点选“删除”命令即可。

保护 CMD 命令行安全

河南 张永夏

打开 CMD 窗口,中可以快速执行各种命令,其操作效率有时甚至优于视窗界面。熟悉系统配置的人都知道,之所以可以顺利执行命令,这其实是“cmd.exe”程序的功劳。正是因为该程序的特殊性,也就成了黑客觊觎的目标。当黑客利用各种漏洞盯上目标主机后,通过各种溢出攻击,就可以调用系统中的“cmd.exe”程序来获得 CMD Shell 控制接口,接下来就可以对系统进行深度入侵了,例如创建非法账户,上传木马等等,因此,对“cmd.exe”程序的使用权限进行合理的管控,对于抗击黑客入侵意义非凡。

利用 NTFS 权限,防止黑客操作 CMD 命令

利用系统的 NTFS 分区的访问控制表(Access Control Lists,即 ACLS),就可以对 CMD 的访问权限进行严格控制。打开“%windir%\system32”文件夹,在其中的“cmd.exe”文件的右键菜单中点击“属性”项,在弹出窗口中的“安全”面板中的“组或用户”列表中依次选择对应的账户,点击“删除”按钮,将所有的账户全部清除。点击应用按钮,在弹出的警告窗口中点击确定按钮,保存设置信息。之后,“cmd.exe”程序就处于禁用状态,不管任何用户试图调用该程序,系统都会弹出“无法访问指定设备,路径或文件,您可能没有合

适的权限访问这个项目”的提示,使其无法操作该程序。

按照同样的方法,对系统路径中的“command.com”程序进行同样的配置,让黑客彻底无法操作命令行界面。当然,为了自己实际需要,也可以创建专用的账户,将其单独添加到“cmd.exe”文件安全面板中的“组或用户”列表中,便于您使用命令行窗口。为了防止 SYSTEM 账户访问“cmd.exe”程序,可以在注册表编辑器中打开“HKEY_CURRENT_USER\Software\Policies\Microsoft\Windows\System”分支,如果没有对应的子键则需要手工建立。在窗口右侧新建名称为“DisableCMD”类型为 DWORD 的项目,将其值设置为“1”,可以禁止命令解释器和批处理文件的运行。经过以上设置,即使黑客对系统进行远程溢出攻击,但是在调用 CMD Shell 接口时会遭到系统拦截,使其无法对获得有效的控制权。

对 CMD 进行完美加密

在默认情况下,任何用户都可以自由的打开 CMD 窗口,但是,在 CMD 窗口中执行各种命令时,有些危险的程序或者命令可能会对系统造成潜在的危害。控制 CMD 窗口的使用权限,为其添加启动密码,是一个比较好的办法。这样当打开 CMD 窗口时,就必须输入预设的密码。这就大大提高了 CMD 窗口的安全性。网上

提供的锁定程序实际上存在很大的漏洞，几乎不堪一击。其实，我们完全可以自己动手，设计一款密不透风的密码认证检测程序，打开记事本，输入以下内容：

```
@Echo off
Setlocal Enabledelayedexpansion
:Test
Echo.
Set/p Pass=Enter Password:
For %%i in ( ^& ^| ^" ) Do (
    Set Pass=!
    Pass:%%i=?! )
If "!Pass!" Equ "opencmd" (
    Echo Password True
    Echo 密码正确欢迎使用命令行
    Pause>nul
    Cmd /k prompt My Commander Line^^^>
) Else (
    Echo Password False
    Pause>nul )
Cls&Goto Test
```

将其保存为“lock.bat”的文件，其原理很简单，就是判断输入的密码是否为“opencmd”，如果是就打开CMD窗口，否则弹出错误提示，当然，您可以根据需要更改改密码。在注册表编辑器中展开路径“HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Command Processor”，在右侧窗口中双击“AutoRun”键值名，将其数值修改为“f:\lock.bat”即可，假设改文件保存在F

盘根路径下，您可以根据进行修改。当打开CMD窗口时，就会自动启动密码验证程序了。该程序的最大特点是可以抗击任意的密码猜测行为，没有正确的密码就别想使用CMD窗口。

为CMD设置专用记录器

当黑客通过某些漏洞对系统远程溢出后，就会利用获得远程CMD Shell接口执行各种危险的命令。了解系统存在哪些安全隐患，将其及时堵上。使用CMD命令记录器，就可以轻松实现上述功能。下载地址：<http://www.greenxf.com/soft/4835.html>。

点击“Win+R”键，执行“cmd.exe”程序，在其中执行“ren c:\windows\system32\cmd.exe cm_.exe”命令，将原来的“cmd.exe”文件更名为“cm_.exe”。如果系统出现文件保护界面，需要点击“取消”按钮，让更名得以顺利进行。也可以在安全模式，WinPE等环境中进行更名操作。将下载的“CmdPlus.rar”压缩包解压到“c:\windows\system32”目录中。将其中的“cmdplus.exe”更名为“cmd.exe”，替换原来的“cmd.exe”程序。之后，如果黑客对本机远程溢得出手，执行的所有命令全部经由“cmdplus.exe”程序，通过匿名管道传送给“cm_.exe”程序去执行，并将其完整记录下来。打开“c:\windows\system32”目录下的“history.txt”文件，可以看到CMD记录信息的所有内容。当然，您自己使用的话，可以直接执行“cm_.exe”程序，来操作各种命令。

莫让远控软件成帮手

河南 刘景云

在日常的工作中，经常会用到各种远程控制软件，让用户可以毫不费力的对远程主机进行控制操作。在系统安全领域，木马对用户的威胁很大。其实，将正常的远控软件和木马进行比较，可以发现两者其实存在一定的共同点。例如，都可以对远程主机进行控制，数据传

输等操作。但是，正常的远控软件以光明正大的身份运行，而木马却是偷偷摸摸的运行，前者帮助用户工作，后者是黑客盗窃用户数据的爪牙。俗话说，善恶只在一念间。黑客不仅仅利用木马对用户主机进行渗透，还将邪恶的目光盯在了正常的远控软件上，于是经过黑客的

“精心改装”，原本正常的远控软件却成了黑客的得力帮手，这不得不引起我们的警惕！

清除暗中潜伏的 Radmin

提起远控软件，Remote Administrator 显得颇有名气。该工具的最大特点是体积精巧，连接速度快，设置简单，操作起来很顺手，成为很多用户的得力工具。俗话说，树大招风。正是因为 Radmin 性能优秀，也成了黑客觊觎的对象。经过黑客的“精心”设计，Radmin 就变成了黑客实现入侵的“利器”。

例如，笔者朋友管理的某台服务器，最近遭到黑客的入侵，其网站主页被恶意修改，嵌入了网马，数据库被破坏，但是经过常规病毒扫描，却没有发现木马或病毒。笔者对其查看，运行“netstat”命令，在网络连接列表中发现 TCP 3389 端口处于监听状态。但是经询问，该机并没有开启终端服务。经过查询该端口关联的进程号，在任务管理器中，发现该服务对应的名称为“r_server.exe”，其对应的用户名为“SYSTEM”，这表明其是由某个系统服务启动的。

看到这里，笔者就明白了，原来这就是 Radmin 这款远控在起作用。朋友告诉笔者，该网站采用的是 PHP+MySQL 结构，因为网站程序设计存在问题，存在注入漏洞，造成黑客利用数据库注入方法，在网站中植入了一句话木马，之后黑客使用专用工具对其进行连接，可以获得具有 SYSTEM 权限的 WebShell 接口，在其中可以随意执行各种命令。当发现网站漏洞后，对其进行了适当的修补，清理了被黑客破坏的网页文件。但是黑客已经通过建立反弹连接，文件上传等手段，将精心伪装的后门程序传送到服务器中并将其激活运行。

在系统目录中经过搜索，发现名为“winregsvr.exe”的文件很可疑，但是对其扫描却发现没有问题。经过检测，这是一个经过特殊处理的 WinRAR 自解压包，但是在其右键菜单中却没有发现“解压到”等项目。将其逆向修复并解压后，发现其中包含“install.bat”，“install.reg”，“r_server.exe”，“rassrv.exe”，“admdll.dll”等文件，打开“install.bat”文件，其内容包含“regedit /s install.reg”，“r_server.exe”，“r_server.exe /silent /install”，“del install.reg”，“del install.bat”等语句，对其中的“install.reg”分析，发现这是一个保存 Radmin 注册表配置信息的文件，当将其悄悄的导入到注册表之后，就会自动完成 Radmin 配置的设置操作，其功能包括将 Radmin 端

口改为 3389，用来迷惑用户，隐藏任务栏图标，添加连接密码等项目。之后的程序语句的作用是隐蔽安装 Radmin 服务，并删除自身文件等。

当 Radmin 远控服务激活后，黑客就可以随时对其进行连接，来控制本机了。不难看出，原本正常的 Radmin 远控软件，到了黑客手里，却变成了入侵工具。因为其本身是合法的程序，所以使用杀软自然无法清除。解决的方法很简单，执行“r_server.exe /stop”命令，关闭 Radmin 远控服务，执行“sc delete r_server”，删除该服务项目，并将上述相关的文件全部删除，就可以彻底关闭 Radmin 远控服务。

被黑客恶意控制的 TeamViewer

在众多的远控软件中，功能最全面强悍的莫过于 TeamViewer 莫属。TeamViewer 具有很多其他远控工具无法比拟的功能，例如，其本身支持 VPN 连接，可以摆脱内网的限制，无需配置反弹连接域名转发等操作，就可以轻松遥控内网主机。正因为如此，其安全性较高，在 VPN 连接中可以保护连接者的 IP 地址。一旦这样的远控利器被黑客恶意利用，其危害无疑是很大的。

例如，笔者同事管理的网站前些天遭到黑客入侵，因为该服务器上运行了 MSSQL 服务器，因为 SA 账户的密码设置的比较弱，加之网页代码存在漏洞，被黑客破译后，通过 Sqltool 等工具执行非法连接，并添加了黑客账户。因为该机开启了终端服务，所以黑客轻易的控制了该机。当发现问题后，管理员立即关闭了终端服务，清除了黑客账户，并修复了各种漏洞。原以为这样就可以避开黑客的袭击，不过，黑客依然可以继续对该机进行非法破坏操作。

笔者分析，黑客一定在该机中留有后门。但是，经过仔细搜寻，例如，查看进程列表，网络连接信息等，都没有发现可疑踪迹。运行 XueTr，在进程列表中发现以红色显示的名为“teamviewer.exe”的隐藏进程，笔者似乎看出了些许端倪。原以为根据其映像路径信息，可以找到目标程序。但是进入对应磁盘后，却无法找到相关的目录和文件。即使在文件夹选项窗口中选择“显示隐藏的文件，文件夹和驱动器”项，取消“隐藏受保护的操作系统文件”项的选择状态，依然无法显示这些文件。

笔者觉得这些可疑程序文件一定被专用的 RootKit 工具处理过，处于隐藏状态。在 XueTr 的“文件”面

板中搜索,才发现其踪迹。因为 Xuetr 运行在 Ring0 级别,可以破解 RootKit 隐藏的文件。经过查看,这些文件其实就是 TeamViewer 的运行文件,只是经过了明显的精简处理,例如删除了“uninstall.exe”,“license.txt”,“unicows.dll”等。很显然,黑客这样做的目的就是为了减小 TeamViewer 的体积。估计黑客没有使用最新版的 TeamViewer,而是采用了版本较低较为成熟的绿色版的 TeamViewer,例如 TeamViewer3.6 等。

同原始的“team viewer.exe”文件相比,黑客使用的“teamviewer.exe”文件体积明显变小,显然黑客使用了 PEexplorer, Rescope 等工具,对其进行了精简,删除了不必要的资源。或者使用加壳工具,对其进行了压缩处理。因为 TeamViewer 的连接密码是不固定的,所以黑客为了便于使用,会设置固定连接密码。例如在 TeamViewer3.6 中,只需在其中点击菜单“额外”-“选项”项,在其中的“常规”选择让 TeamViewer 自动运行,并设置连接密码,黑客就可以顺利连接被控机。为了保证 TeamViewer 稳定运行,可以在“安全”面板中禁止关闭 TeamViewer,或者让管理员用户才可以更改配置信息。通过在“入站访问控制”栏中选择“完全控制”项,黑客就可以彻底控制被控机。

TeamViewer 具有导出配置信息的功能,可到便于黑客导入导出配置信息。例如黑客可以在本机上配置好 TeamViewer 各项参数,之后在被控机上直接导入,就可以完成配置操作。即使是内网主机,利用 TeamViewer 内置的 VPN 连接工具,黑客也可以轻松创建 VPN 功能,让其和黑客主机处于 VPN 虚拟网中,遥控起来毫不费力。根据以上分析,黑恶的入侵手法是先通过各种漏洞,通过终端服务控制目标机,为了实现稳妥的远控操作,避免管理员发现入侵痕迹后关闭终端服务,导致入侵无法进行,因此黑客将精心配置的 TeamViewer 传送到该机上。这样,即使终端服务被关闭,黑客照样可以利用隐藏的 TeamViewer 来远控本机。为了隐蔽运行,黑客会借助于 AFX Windows Rootkit 等工具,对其 TeamViewer 的存储目录进行 RootKit 隐藏处理,之后隐形运行 TeamViewer,不仅其存储位置无法被用户发现,而且其进程,端口,注册表信息也处于隐藏状态难以发现。

这样,当管理员关闭了终端服务后,黑客依然可以利用潜伏的 TeamViewer,来对被控机进行遥控。了解了黑客的手法后,可以在 XueTr 中强制关停 TeamView 进程并删除关联文件,并在其文件面板中删除强制删除相关文件,彻底关闭黑客开启的后门。



无线路由安全不容忽视

江苏 陈沪娟

伴随着智能终端设备的不断普及,越来越多的单位用户开始使用无线路由器,来在局部范围部署无线网络。不过,无线路由器常常会因为固件 BUG、设置错误、系统漏洞等因素,引起一些安全问题,要是这些问题被恶意用户利用,便很有可能会造成无线路由器被非法攻击,甚至这些恶意用户可以通过入侵的无线路由器,威胁整个无线网络的运行安全。为了保证整个无线网络安全,我们必须高度重视无线路由器的一些安全细项,避免它们成为安全“短板”。

更新固件程序

众所周知,与普通计算机相似,无线路由器的固件程序相当于 BIOS 软件,它事先已被固化到路由器设备主板芯片上,往往用来控制和协调路由器内部集成电路的。正常来说,无线路由器工作一段时间后,固件程序自身存在的编程错误、软件 BUG 等现象,会被逐渐发现,一旦它们被恶意用户非法利用,那么无线路由器就会成为“肉鸡”,恶意用户利用它能轻松攻击无线局域网中的其他计算机甚至服务器。所以,为了堵住安全漏洞,设备生产厂商都会在官方站点上,及时发布新的固件版本,来修复存在的安全问题。对于普通用户来说,只要

定期到网上下载安装最新版本固件, 及时对无线路由器后台系统进行升级更新, 就能让设备在高效运行的同时, 不会轻易遭遇恶意用户的攻击。

对无线路由器固件程序进行升级, 实际上就是用高版本替代当前低版本的常规更新操作。在获取高版本固件程序时, 首先应该检查无线路由器的铭牌信息, 记下设备的品牌和型号内容, 根据这些内容进入指定路由器设备的官方站点。比方说, 当终端用户查找到无线路由器是 TP-Link 品牌时, 只要开启 IE 浏览窗口, 在该窗口地址栏中输入对应品牌的官方 URL 地址 “http://www.tp-link.com.cn”, 进入如图 1 所示的浏览页面。选中并点击该页面中的“无线网络产品”链接, 在对应链接页面中找到特定型号的无线路由产品, 点击该产品页面中的“相关下载”按钮, 从下载页面中下载得到最新版本的固件程序和有关升级程序, 将它们一起存储到本地计算机硬盘中。



图 1 浏览页面

之后通过双绞线将本地计算机与无线路由器连接在一起, 启动运行计算机系统上的 IE 浏览器程序, 在浏览窗口中输入无线路由器默认的 Web 管理地址, 打开路由器后台管理登录页面, 输入管理员账号, 确认后登录进入后台系统管理页面。从中先找到备份功能选项, 指定好备份文件存储路径, 将无线路由器当前的配置参数备份保存好, 避免固件升级操作失败引起的配置丢失现象。接着找到“固件升级”功能, 打开新版本固件上传页面, 添加并导入已经获得的新版本固件程序, 执行“升级”命令进行固件程序的更新操作。更新操作结束后, 将先前已经备份好的路由器配置信息快速还原, 这样就能增强无线路由器自身的安全防范能力了。

要提醒大家的是, 进行无线路由固件程序更新操作时, 必须要注意一些细节事项: 首先在固件程序更新过程中, 千万不能断开电源, 否则的话无线路由器可能会受到损坏。其次要将所有处于运行状态的应用程序都退出, 特别是要将屏幕保护程序和杀毒软件退出, 避免固件程序更新操作受到它们的干扰。第三尽量从无线路由

器官方网站中下载固件程序和刷新升级工具, 同时确保固件版本要与无线路由器的型号信息保持一致。

修改账号密码

不少用户将无线路由器购买回来后, 往往直接接入网络开始使用, 很少有人会主动修改无线路由器的配置参数, 甚至连缺省的管理员帐号和密码也懒得去修改, 这就为恶意用户的非法入侵带来了机会。即使有用用户修改了无线路由器后台系统的默认密码, 但是这些用户在修改密码时, 为了图方便、好记忆, 往往喜欢用电话号码、生日、纪念日或几位连号数字、重复数字作为密码内容, 甚至经常用几个固定的数字作为不同系统的登录密码, 显然这种做法是不可取的, 因为这些简单的密码被暴力破解的成功率很高。非法用户可以使用常见的 root、guest、admin 等帐号与密码, 来进行试探性登录, 也可以使用专业工具来进行暴力破解性登录, 一旦无线路由器被入侵, 那么本地无线网络将会不可避免地成为“肉鸡”。

修改无线路由器登录密码时, 最理想的密码内容组合是连用户自己都不熟悉规律的密码, 密码没有规律可循, 自然破解起来也就不那么容易了, 比方说同时包含大小写字母、阿拉伯数字以及特殊符号的密码内容, 被成功破解的机率相当低。此外, 无线路由器登录密码最好应定期修改, 千万不能为了图省事, 将密码信息记在无线路由器外壳身上, 或者其他特别显眼的地方。

在进行帐号密码修改操作时, 可以先进入无线路由器后台管理页面, 将鼠标定位到“系统工具”、“修改登录口令”节点上, 在对应选项设置区域, 输入原始帐号名称和密码, 再输入新帐号名称和密码, 单击“执行”按钮就能让新帐号生效了。当然, 有些无线路由器登录密码分为管理员、普通用户等不同级别, 其中管理员级别可以访问无线网络各种参数设置, 还能对参数自由编辑修改, 普通用户级别只能访问无线网络的参数设置, 无法对其自由编辑修改。所以, 用户必须要根据实际情况, 来合理定义好不同级别的登录密码, 确保无线路由器登录安全。

调整远程端口

为了便于对无线路由器的管理维护, 不少用户会在路由器的 Web 设置页面, 勾选远程登录该设备的允许

选项,可是远程 Web 登录功能在缺省状态下会使用“80”端口,这个端口号码经常会被恶意用户非法利用,不利于无线网络的安全稳定运行。

要想避免无线路由器被非法远程攻击,我们不妨尝试将缺省的远程管理端口调整为一个不经常使用的号码,日后只有熟悉新端口号码的用户,才能通过 Web 页面远程登录进入无线路由器来对远程管理维护。比方说,要将 Web 管理端口调整为“5633”时,只要先打开无线路由器后台管理界面,依次展开“安全设置”、“远端 Web 管理”节点,在指定节点选项设置区域,将“Web 管理端口”参数调整为“5633”,再在“远端 Web 管理 IP 地址”设置项处,指定好能对无线路由器进行远程管理维护的计算机 IP 地址,按下“保存”按钮执行设置存储操作,最后重启无线路由器设备。这样,日后只有在特定计算机上,输入无线路由器的 IP 地址和新端口号码,才能对其进行远程管理维护操作。

当然,无线路由器还隐藏了 Telnet 这种远程登录方式,这种登录方式常常被用户所忽视,实际上该登录方式大量应用在网络的网关设备和重要主机中,它也能成为网管员提供远程维护通道。但是该远程功能使用的是“23”端口,该端口也是一把“双刃剑”,如果被非法用户利用时,同样会给无线路由器带来安全麻烦。非法用户只要使用专业工具对本地网络进行扫描,要不了几分钟,就能扫描到无线路由器开放着的“23”网络端口。

一旦看到该端口处于开放状态时,我们必须想办法将其及时关闭,或者将其修改为陌生的端口号码。当然,有的无线路由器可以通过更新固件程序的方法,来修复这种安全问题,用户只要及时到设备官方网站下载更新固件,就能保证远程维护的安全。

预防网页劫持

用户在网上冲浪过程中,我们经常会碰到网页劫持现象,对于这种现象,使用一些专业的反劫持插件程序,能够避免大多数网页劫持现象,不过对于那些来自网络运营商的广告劫持,反劫持插件程序就无能为力了。现在只要进入无线路由器后台管理页面,修改有关功能参数,就能预防网络运营商的网页劫持了。例如,对于 TP-Link WR541G/542G 无线路由器来说,可以进行如下设置操作,来拒绝网页劫持现象:

首先在 IE 浏览窗口地址栏中,输入无线路由器 Web 访问地址,登录进入该设备后台管理页面,依次展

开“安全设置”、“防火墙设置”节点选项,选中对应选项设置区域中的“开启防火墙”选项,同时将“开启域名过滤”也勾选起来(如图2所示),按下“保存”按钮执行设置保存操作。

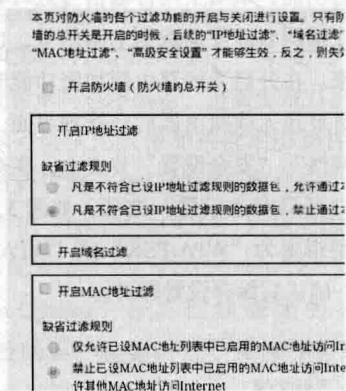


图2 设备后台管理页面

接着将鼠标定位到“安全设置”、“域名过滤”节点选项上,按下对应选项设置区域中的“添加新条目”按钮,将网络运营商广告域名填写到“域名”位置处,比方说输入“search.114.vnet.cn”、“114.vnet.cn”等广告域名。再将“生效时间”定义为“00-24”,将状态参数修改为“生效”,按下“保存”按钮退出设置操作。要是不清楚网络运营商的广告域名,不妨在 IE 浏览界面中随意输入一个不正确的网站域名,记录下随后出现的劫持页面地址,将该地址填写在域名过滤列表中。

要想过滤特定劫持页面 IP 地址时,不妨先通过 ping 命令测试网络运营商的广告域名,将回显出来的 IP 地址记忆下来。再进入无线路由器 IP 地址过滤页面,单击“添加新条目”按钮,在“广域网 IP 地址”设置项处,输入先前记录的 IP 地址,同时将“生效时间”指定为“00-24”,将状态参数调整为“生效”,将协议参数选择为“All”,将“通过”参数设置为“禁止通过”,按下“保存”按钮存储好设置操作,最后重启无线路由器设备。

当我们再次上网访问时,网络运营商的广告域名和相关 IP 地址都会被正确过滤了,日后 IE 浏览页面自然就不会发生被广告劫持现象了。如果网络运营商修改了广告链接地址,只要按照之前的操作步骤,将变化的广告域名和 IP 地址输入到过滤列表中即可。同样地,我们可以将其他的劫持页面域名和 IP 地址输入到无线路由器过滤列表中,以达到预防恶意页面劫持的目的。

拒绝他人蹭网

在使用无线路由器组网的环境中，蹭网现象越来越普遍。为了避免这种现象，我们可以启用无线路由器的上网信号加密功能，来对上网传输信号进行非常复杂的加密计算，让蹭网者即使窃取到上网信号，也很难将它成功破解开来。在开启无线路由器加密功能时，不妨先以系统管理员登录无线路由器后台管理界面，将鼠标定位到“无线网络”、“安全设置”节点上，在对应节点设置区域选中“开启安全设置”选项（如图3所示），同时将安全类型指定为“WPA-PSK”或“WPA”，再输入好密钥内容，确认后保存设置即可。

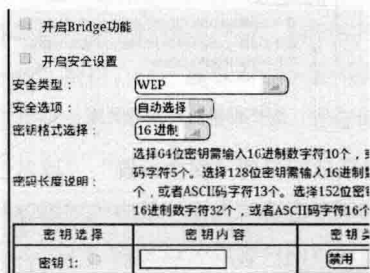


图3 开启安全设置选项

对于已经成功蹭网的用户，该如何将他们揪出来呢？使用“WifiChannelMonitor”这款工具，配合无线路由器自身的MAC地址过滤功能，就能将危险的无线网络蹭网者寻找出来，并拒绝他再次蹭网。因为“WifiChannelMonitor”工具是利用微软的网络监视器来监控无线网络流量的，在利用该工具检测蹭网现象之前，必须先从微软官方站点下载安装“Microsoft Network Monitor”工具，再开启“Wifi ChannelMonitor”程序

的运行状态，进入对应程序主操作界面。按下“Start Capture”工具栏按钮，选择需要监控的无线网卡设备，定义好无线网络通道参数，确认后让程序切换到检测状态。被探测到的无线网络信号会自动显示在对应程序列表中，将绿色图标的无线信号选中，这时用户能发现所有与该无线网络相连的设备。用鼠标双击某个设备名称，在其后界面中能查明设备的客户端类型、数据字节、MAC地址、设备制造商等信息，根据设备制造商信息就能识别出当前连接的设备是否属于自己所用的上网设备，如果不是的话，那该设备自然就是蹭网者了。

一旦识别出蹭网者所用设备后，重新进入“WifiChannelMonitor”程序主界面，从中找到对应设备的MAC地址，同时将其记录下来。

之后进入无线路由器的后台管理界面，从中找到并启用“MAC地址过滤”功能选项，在对应选项的设置页面中（如图4所示），输入蹭网者的设备MAC地址，确认后保存设置操作，这样就能拒绝他再次蹭网了。

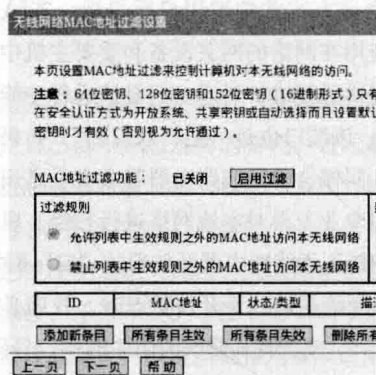


图4 对应选项的设置界面

让木马无法藏身启动项

河南 张永夏

木马除了伪装成服务启动之外，将自身隐藏于注册表中众多的启动项目中，跟随系统自动运行，也是木马最常用的招数。由于注册表中和启动项相关的实在太多，这里不可能逐一介绍。手工在注册表中逐一查询毕

竟过于繁琐，其实，使用 AutoRuns 这款强悍的安全软件，就可以将几乎所有的启动项一网打尽，包括系统登录，网络服务，打印监控，安全认证，网络连接，系统服务，驱动程序，解码组件，引导执行，映像劫持，初

始程序,计划任务,动态链接,IE 浏览器,资源管理器,登录等十多个和启动项紧密相关的类型(如图1所示)。在每个类型中包含了相应的启动项目。如果打开“所有项目”面板,可以浏览所有的启动项目。不管木马在注册表启动项中隐藏的有多深,都会在 Autoruns 面前彻底暴露,选择和木马相关的启动项,在其右键菜单中可以执行删除,定位注册表具体路径,打开目标文件夹,在线查询,管理目标进程(必须安装有 Process Explorer 这款软件强悍的进程管理软件)等操作。



图1 使用 AutoRuns 分析启动项

值得注意的非常规启动位置

当然,对于狡猾的木马来说,绝不会采用在诸如“HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Run”等“显眼”的位置藏身,毕竟这样做太容易暴露。例如对于采用进程插入技术的DLL木马来说,注册表中“HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows NT\CurrentVersion\Windows”下的“AppInit_DLLs”键值是其很好的藏身地,该位置是很容易被大家忽视的可以用来启动木马的位置。如果DLL木马对其进行修改,将自身添加进来,那么不管任何进程,只要其使用到了“User32.dll”动态库,都会被上述键值指向的DLL木马所注入。因为“User32.dll”是系统自带的很常用的动态库,主要用来提供和程序使用界面,消息控制等相关的功能,几乎被大多数程序使用。当然,只有极少数程序(诸如CMD控制台)是不会使用该动态库的。此外,注册表中的“HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Policies\Explorer\Run”分支也应引起我们的关注,这个组策略中的启动项目紧密相关的。为了避人耳目顺利启动,木马还常会在注册表中的“HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows NT\CurrentVersion\Winlogon”分支下的“userinit”和“shell”键值中添加恶意程序,悄无

声息的跟随系统启动自动激活。

对于国外的木马来讲,通常会利用 ActiveX 技术来自启动。例如比较有名的 Beast 木马,会在注册表中的“HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Active Setup\Installed Components\{4A202188F04D-11CF-64CD-31FFAFECECF20}”分支下的“StubPath”键值中设置木马程序路径,进而实现自启动操作。有些狡猾的木马会采用映像劫持技术绑架特定程序,当用户执行该程序时,运行的却是木马程序。如果采取将注册表中的“HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows NT\CurrentVersion\Image File Execution Options”分支彻底删除的方法,来防御映像劫持的话,就显得过于简单了,因为从编程角度看,木马程序通常会使用 RegCreateKeyEx() 和 RegSetValueEx() 等函数,来动态的创建或者修改注册表键值数据。

因此,为了有效防御映像劫持,可以采取控制上述注册表路径权限的方法,取消“Administrators”组和“SYSTEM”账户对该分支的写权限,具体的方法比较简单,这里就不赘述了,这样木马就无法凭借映像劫持来启动了。

为启动项和服务安装“监控器”

实际上,现在的安全软件(例如金山卫士,360安全卫士等)都可以对启动项和系统服务进行监控,当发现这些位置有风吹草动的话,就会弹出提示框,让用户决定是否运行相关的操作。如果您想更加彻底的保护启动项和服务,还可以使用 Ghost Security Suite 这款软件,来执行更加严格的监控操作。

Ghost Security Suite 内置的大量安全规则,已经涵盖了所有的启动项和系统服务列入监控范围,无需您的任何干预。当可疑程序试图修改或者创建启动项或者系统服务时,必然涉及对相关注册表项的改动, Ghost Security Suite 可以立即对其拦截,在弹出的警告窗口中的“1.This Application”面板中显示程序名称,在“Whats to perform this action”面板中显示修改动作,在“Key”栏中显示该程序要修改的注册表主键名,在“Value”栏中显示建立的键值名称,在“Value Data”栏中显示该程序所在的路径信息。

根据其提供的详细的信息,您很容易判断其目标程序的真实身份。对于正常的程序,点击“Allow”按钮

放行即可。对于非法的程序,最好点击“Block”按钮,拦截其对注册表中服务配置项目的修改。如果在询问窗体左上角的模式列表中选择“Advance Alert”项,在高级询问窗体中可以显示更加细致的内容,除了上述描述信息外,还包括可疑程序的原始运行路径、触发规

则所监控的注册表路径、规则所属组名等内容。

如果确认是可疑程序,还可以直接点击“Kill Process”或者“Kill Thread”按钮杀死对应进程或线程。这样木马还没有来得及对启动项或者服务下手,就会被 Ghost Security Suite 彻底清除。

实战攻防 TCP/IP 筛选策略

河南 郭建伟

在网络环境中,电脑和外界进行通讯依靠的是本机开放的网络端口。现在的病毒、木马、黑客软件之所以能够在网络中兴风作浪,就是利用特定的网络端口进行非法活动的。利用 Windows XP 的 TCP/IP 筛选策略,可以轻松关闭各种危险端口,从而有效地切断黑客入侵、病毒传播的途径。使用 TCP/IP 筛选器的最大优点是可以有针对性的开放端口,这样不需要的端口就自动封闭。

设置 TCP/IP 筛选策略

打开本地连接的属性窗口,在“常规”面板中双击“Internet 协议(TCP/IP)”项,在弹出的窗口中点击“高级”按钮,接着打开“选项”面板,在其中双击“TCP/IP 筛选”项,在“TCP/IP 筛选”窗口中勾选“启用 TCP/IP 筛选”项,本例中根据需要在“TCP 端口”、“UDP 端口”和“IP 协议”栏中勾选“只允许”项,点击“添加”按钮,依次输入允许开放的端口即可,点击确定按钮保存设置,然后重新启动系统即可。

黑客如何破解 TCP/IP 筛选策略

使用了 TCP/IP 筛选策略封闭危险端口后,就可以高枕无忧了么?实际情况未必如此。TCP/IP 筛选策略的配置信息实际上保存在注册表中,只要对注册表对应的项目进行简单的修改,就可以轻松解除 TCP/IP 筛选策略的封锁。

假设在 TCP/IP 筛选策略只开启了“3389”端

口。在“开始”→“运行”中执行“Regedit.exe”程序,在注册表编辑器中展开“HKEY_LOCAL_MACHINE\SYSTEM\ControlSet001\Services\Tcpip\Parameters”分支,在右侧窗口中双击“EnableSecurityFilters”键值名,在打开的对话框中可以看到其数值为“1”,表示已经启用 TCP/IP 筛选策略,如果将其值设为“0”,即可关闭 TCP/IP 筛选策略。例如,当黑客通过各种漏洞或者非法提权操作获得 CMDshell 控制环境后,可以使用系统自带的“reg.exe”程序,对上述注册表路径进行改写,来突破 TCP/IP 筛选策略。

此外,展开“HKEY_LOCAL_MACHINE\SYSTEM\ControlSet001\Services\Tcpip\Parameters\Interfaces\{E18633C4-C26E-4A34-8CA6-B7B5BE452C8D}”分支,注意其中的 CSID 项根据不同的电脑而定,在右侧窗口的“TCPAllowedPorts”、“UDPAllowedPorts”和“RawIPAllowed Protocols”键值名中分别保存着允许开放的 TCP、UDP 和 IP 端口列表,如图 1 所示。知道了 TCP/IP 筛选策略的保存机理,入侵者就完全可以设计出一个针对 TCP/IP 筛选策略的木马程序,首先将“HKEY_LOCAL_MACHINE\SYSTEM\ControlSet001\Services\Tcpip\Parameters”路径单独导出,然后将上述注册表路径中的“EnableSecurityFilters”键值名的值设置为“0”,即可禁止 TCP/IP 筛选策略,同时将遍历上述注册表分支中的“Interfaces”下的所有子键,将其中的“TCPAllowedPorts”、“UDPAllowedPorts”和“RawIPAllowed Protocols”键值名清空,即可开放所有端口。这样,当黑客完成入侵动作后,再将先前保存

的注册表路径导入（例如使用“regedit s c:tcpip.reg”，假设 tcpip.reg 为导出的文件），即可悄无声息地突破攻破 TCP/IP 筛选策略的封锁了。



图 1 查看保存在注册表中允许开放端口列表

彻底保护 TCP/IP 筛选策略

从上面的分析可以看出，启用了 TCP/IP 筛选策略后，不要以为系统就此彻底安全了。要想保护 TCP/IP 筛选策略配置信息，必须从保护注册表中的相关配置项目入手。我们前面谈到，黑客会利用系统自带的“reg.exe”程序，来对目标注册表数据进行修改。那么最好的方法就是将“C:\Windows\System32”文件夹中的“reg.exe”彻底行删除，实际上我们平时也很少使用到该程序，将其删除对日常操作几乎没有影响。当然，还可以利用权限配置功能，来限制其他用户对上述敏感键值的读写操作。例如，运行“regedt32.exe”程序，在注册表编辑器中选择“HKEY_LOCAL_MACHINE\SYSTEM\ControlSet001\Services\Tcpip\Parameters”分支，在其右键菜单中点击“权限”项，在权限设置窗口中禁用所有账户（包括 Administrators 组等），对该分支的完全控制和读取权限，这样黑客就无法使用“Reg.exe”程序，来随意读写其中的数据了。

当然，还可以使用各种注册表监控软件，来密切监视和 TCP/IP 筛选策略关联的注册表数据变化，来及时获得报警信息。这样的软件有很多，这里就以 Ghost

Security Suite (以下简称 GSS) 这款强悍的注册表保护工具为例, 来保护指定的注册表路径。在 GSS 主窗口顶部点击“注册表保护”按钮, 在规则配置窗口(如图 2 所示)左侧列表选中合适的类别, 在右侧的“组名称”栏中输入新的组名, 在“组描述”栏输入描述信息, 点击“添加组”按钮建立新组。随后在左侧列表选中新建组名, 点击规则列表中的“添加规则”按钮, 在新建规则窗口中的“步骤 1- 注册键”栏中选择上述注册表路径, 在“步骤 2- 注册值”栏中选择该主键下的具体键值。注意, 主键和键值的设定都支持“*”, “?”, “~”三种通配符, 这将极大提高防御的灵活性。* 代表任意字符串, ? 代表单个字符, ~ 代表只匹配当前一层注册表项, 遇到“\”则中止。~ 经常与 * 搭配使用。例如: HKEY_LOCAL_MACHINE\Software*~ 与 HKEY_LOCAL_MACHINE\Software\Ghost Security 匹配, 与 HKEY_LOCAL_MACHINE\Software\Ghost Security\RegDefend 则不匹配。最后点击“添加规则”按钮保存设置。



图 2 GSS 规则配置界面

之后在配置窗口的中选中该新建规则，在下面的“1. 在这些事件”栏中可以组合选择读取键、创建键、修改键、读取键、设置键、删除值等保护项。在“2. 执行这些操作”栏中设定当满足此条规则时，执行的动作类型，包括拦截，记录到磁盘、询问用户等。例如，在本规则可以选择拦截动作，这样当有程序试图修改对应的注册表键值时，GSS 即可对其进行拦截。



交换机安全由配置把关

河南 郭建伟

单位网管员在管理维护网络的时候，总需要接触到交换机设备，该设备是局域网中的核心设备，它的可靠性和安全性直接决定着整个网络的运行稳定性。所以有效地管理配置好交换机，是确保单位局域网运行安全和可靠的关键。然而，面对着风起云涌的黑客入侵和疯狂肆虐的病毒攻击，交换机自身的安全性正变得越来越脆弱。现在本文就从配置着手，来增强交换机的安全运行性能，从而让其发挥保护网络的作用。

配置密码保护

大家知道，管理员通过交换机管理网络时，常常会从 Console 连接端口登录该设备后台系统。默认状态下，交换机后台系统不会要求用户输入登录密码的，这显然是非常不安全的。为了保护交换机后台系统用户界面的登录安全，我们应该为 Console 连接配置登录验证密码。例如，要为思科交换机的 Console 端口配置密码保护时，可以在后台系统依次执行“line con 0”、“password xxx”、“login”等命令即可。这种方法只能设置明文密码，别人在后台系统执行“show run”命令，可以查看到“password”的具体内容。为了让密码保护更加安全，建议大家可以使用“service password-encryption”命令，对明文密码内容执行加密操作，甚至可以使用“enable secret yyy”命令，启用强加密的特权密码。为了改善配置效率，不少网管员也会通过 telnet 命令对交换机进行远程配置。当然，要是启用了 telnet 登录功能后，一些恶意用户或许会趁机利用该功能，悄悄登录进入交换机后台系统，对局域网中的许多关键配置进行恶意修改，引起网络不能稳定工作或发生安全事故。为此，我们应该加强用户界面的登录验证配置，强制用户在 telnet 登录交换机时进行身份验证，具体操作命令包括“line vty 0 4”、“password xxx”、“login”等。

对于 H3C 系列交换机来说，它们支持 password、scheme 等加密认证方式。比方说，要强制管理员以

telnet 方式管理交换机必须进行登录认证时，比方先在交换机后台系统全局模式下，通过“user-interface vty0”命令切换到 vty0 用户界面视图状态，继续输入“authentication password”命令，开启远程登录认证功能。当成功启用了该功能后，还需要使用“set authentication password simple xxx”命令来指定登录密码，这里的“xxx”为具体的明文口令内容，比方说输入“set authentication password simple 123456”命令，就意味着将远程登录认证口令设置成“123456”。倘若强制 telnet 用户同时进行用户名和口令验证时，必须在用户界面视图模式状态下，执行“authentication-mode scheme”命令，来将远程用户名和口令认证功能启用起来，这样日后从 vty0 用户界面登录配置交换机时，系统就会强制用户输入具有合法权限的用户名和密码。例如，要强制远程 telnet 用户从 vty0 用户界面登录交换机，一定要使用“123”账号、“456”口令时，不妨在交换机后台系统全局模式状态下依次执行如下命令：

```
user-interface vty0
authentication-mode scheme
quit
local-user 123
password simple 456
service-type telnet
```

配置环路保护

为了改善传输稳定性，不少单位网络都采用了冗余连接，对物理线路进行备份。然而，这种连接方式从物理连接角度来看，已经在单位网络中构成了物理环路，该环路在 stp 协议的支撑下，不会影响网络信号的正确传输；不过，在长时间工作过程中，单位网络会受到工作环境、人为操作、设备质量等因素影响，或许会发生网络环路故障，而从平时的实践工作来看，这种环路故障很容易出现在交换机调整的位置。要是物理环路真的

构成网络回路，那么交换机端口很快会被大流量信号堵塞，单位网络的运行自然就会受到严重影响。为了保护交换机安全，改善网络传输稳定性，我们不妨配置启用交换机的环路保护功能，让其智能识别特定端口下出现的网络回路现象，同时自动停用出现网络回路的交换端口，并且及时上报相关日志内容，日后我们根据设备日志内容就能快速找到故障原因，让单位网络迅速恢复到正常状态。

以 H3C 系列交换机为例，在配置环路保护功能时，只要在交换机后台系统的全局视图模式下，输入“interface e0/26”之类的命令，进入目标交换端口视图模式，使用“display loopback-detection”命令，先查看指定交换端口在当前有没有配置端口回路监测功能（如图 1 所示），而且该命令还能查出该端口下有没有回路现象存在。倘若看到网络回路监测功能还没有被开启时，不妨输入“loopback-detection enable”命令，来达到开启目的。日后要是想临时关闭这项功能时，可以再使用一次“undo loopback-detection enable”命令。

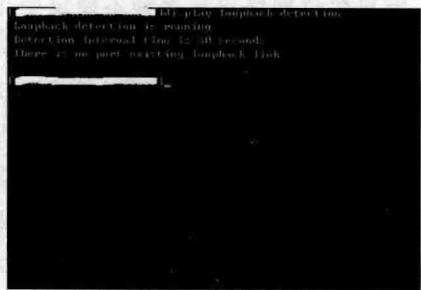


图 1 未配置回路监测

在缺省状态下，配置好的交换端口环路保护功能只会对当前端口下面的默认 VLAN 有效，要想对当前端口下的所有 VLAN 都有效时，必须要执行“loopback-detection per-vlan enable”命令，让网络环路保护功能自动检查当前端口下的所有 VLAN。此外，指定交换端口要是处于 Access 工作模式，那么网络环路保护功能即使扫描到了当前端口下的网络回路，也不会向交换机后台系统自动报告日志信息，只是简单地关闭当前交换端口的工作状态，避免网络回路影响到整个单位网络的正常运行。要是交换端口工作在 Trunk、Hybrid 模式，那么网络环路保护功能扫描到当前端口下存在网络回路时，立即会以日志形式向系统报警，但不会关闭当前端口的工作状态，倘若要关闭交换端口运行状态时，只要输入“loopback-detection control enable”命令，配置好网络回路监测受控功能即可。

配置服务保护

交换机的许多功能都是以服务形式存在，开启的服务越多，表示交换机可以支持的网络功能越多。但对特定用户来说，并不是交换机的功能越多越好，因为那些平时很少用到的网络功能，不但会消耗交换机后台系统的宝贵资源，而且会容易引起安全麻烦，从而影响整个单位网络的运行稳定性。因此，我们可以及时关闭不需要的服务，确保交换机只使用有限的几个网络功能。

例如，在 Cisco 交换机环境下，如果不希望用户通过网页浏览方式，远程查看交换机后台管理配置页面时，只要在后台系统配置状态下，执行字符串命令“no ip http server”即可。这时，恶意程序将无法不停地向局域网交换机发送 HTTP 请求，那么交换机就用不着不停地消耗系统资源进行应答，自然也不会引起交换机发生瘫痪现象，局域网上网将会始终安全稳定。如果不希望交换机使用 Chargen、Discard、Echo 之类小的 udp 服务时，可以执行“no service udp-small-servers”字符串命令，来临时关闭小 udp 服务的运行状态。同样地，使用“no service tcp-small-servers”命令，可以让交换机临时关闭 Daytime、Chargen、Discard、Echo 之类小的 tcp 服务。为了避免网络中的恶意程序进行路由欺骗攻击，管理人员可以执行“no ip source-route”命令，暂时关闭交换机中的 IP 源路由功能，以便强制其丢弃带源路由选项标记的数据包。

配置流量保护

在单位网络环境中，因为终端用户任意下载，引起网络带宽资源被过度消耗的现象经常发生。为了避免这类现象的不断发生，管理员可以通过配置交换机的流量控制功能，来对网络流量的使用进行保护，一旦看到当前交换端口下面存在异常网络流量现象，流量控制功能就会智能向当前交换端口发送报警消息，通知远端上网端口暂时不要继续向当前交换端口发送数据信息，以防止网络流量进一步堵塞交换机现象。而对端上网端口要是接收到报警信息后，会临时暂停向当前交换端口发送数据，这么一来就能有效避免数据信息发生丢失现象了。

以 H3C 交换机为例，在将当前交换端口的流量控制功能配置起来时，一定要先登录交换机后台系统，输入“system-view”命令，进入后台系统全局视图模式状态（如图 2 所示），接着通过“interface e0/2”之类命令，进入

当前交换端口的视图模式状态,继续输入“flow-control”命令并回车,那么当前端口的流量保护功能就被配置成功了。当然,默认状态下,交换机下的所有网络端口并没有开启流量控制功能,管理员必须依照实际情况来使用这种功能。如果日后某个交换端口不需要进行流量保护时,只要进入该交换端口视图模式状态,输入“undo flow-control”字符串命令,再保存设置操作,关闭流量管理功能就 OK 了。



图 2 进入后台系统

配置 VTP 协议保护

大家知道,VTP 协议是思科交换机独有的一种网络协议,其中文名称为虚拟局域网中继协议,它的功能主要是向单位网络中的所有交换机,自动广播虚拟局域网配置数据,确保网络运行维护更加快捷方便。就该网络协议来说,交换机能分成 VTP 客户端、VTP 服务器这两大类,其中 VTP 客户端主要用来接受来自服务端的各种声明和通知,VTP 服务器主要用来发送所有的虚拟局域网配置数据。当管理人员每次调整 VTP 服务器的配置信息时,例如修改 VLAN 属性信息,甚至直接删除或添加 VLAN 时,VTP 配置版本号就会自动加 1,借助大小不一的配置版本号,VTP 客户端可以实现与 VTP 服务器配置信息的同步。利用这个特点,恶意用户常常会伪造一台配置版本号大的 VTP 服务器,连接到单位网络中,这时网络中其他的 VTP 客户端在发现伪造 VTP 服务器的“身影”后,会智能用虚假配置数据直接覆盖原先正确的配置数据,这样单位网络就会受到非法攻击。

为了防止恶意用户使用 VTP 协议攻击网络,在组网规模大的环境下,管理人员可以停用交换机的 VTP 协议,也可以启用 MD5 验证方式,加密保护所有的 VTP 配置数据,确保其他 VTP 客户端不同步 VTP 配置数据,要是配置数据中包含的加密信息不正确时,其他 VTP 客户端自然不能与 VTP 服务器同步。要为网络的 VTP 服

务器配置加密保护时,不妨先切换到特定 VLAN 视图模式,在该模式下逐一输入“vtp domain xxxxxx”、“apply”、“exit”等命令即可,这里的“xxxxxx”就是 VTP 域的保护密码。完成上述设置任务后,恶意用户日后就不能进行 VTP 协议攻击,将所有非默认的 VLAN 从 VLAN 数据库中删除掉了。

配置 Root 地位保护

正常情况下,普通生成树根桥和备份交换机要同处相同域中,但对内部生成树来说,生成树根桥和备份交换机往往会被管理人员放置在核心域内。这时网络要是遭遇到恶意攻击,或者管理人员工作失误,网络中的有效根交换机就容易接受到更高优先级的广播配置消息,这样有效根交换机 Root 地位将会自动丧失,从而引起整个网络组网结构发生错误变化。这时,本来应该从主干网上传输的网络流量,会被自动牵引到普通传输链路上,最终造成整个网络传输通道堵塞现象。

为了防止单位网络出现这种不稳定变化,H3C Quidway S8500 核心交换机允许组网用户配置 Root 保护功能,来维持根交换机的地位。当某个交换端口配置了 Root 保护功能后,日后对应端口在所有实例上的端口角色,都会被智能选择为当前端口;倘若这种类型交换端口从单位网络中接受到更高访问级别的配置消息时,它的端口角色仍然是当前端口,只是它的工作状态会调整为侦听状态,不再支持数据报文转发功能。在保持一段时间后,如果这种类型交换端口一直没有从单位局域网中,接受到更高访问级别的配置消息时,它的工作状态就会被自动恢复到缺省状态。

在缺省状态下,S8500 核心交换机端口没有配置 Root 保护功能。如果要为特定交换端口配置这项功能时,不妨先切换到交换机后台系统,通过“system-view”命令,进入系统视图模式,再在该状态下使用“interface xxx”命令进入指定交换端口视图(“xxx”为特定交换端口),在该视图模式下输入“stp root-protection”字符串命令即可。日后不想使用 Root 保护功能配置时,只要简单地输入“undo stp root-protection”命令就行。

如果想提高操作效率,将多个交换端口配置成 Root 保护时,只要通过“stp interface interface-type interface-number [to interface-number] &<1-10> root-protection”命令即可。

❖ DHCP 上动手脚，安全有保障

江苏 孙秀洪

大家知道，DHCP 服务器主要作用就是为上网计算机，动态分配 IP 地址、默认网关、DNS 等参数，提高它们网络连接效率的。如果我们能够拓宽思路，在 DHCP 服务器对外服务的过程中，灵活加入一些安全控制设置，不但能够获得较高的网络接入效率，而且能够获得良好的安全保障效果，让局域网上网安全又高效。现在，本文就在 DHCP 服务器中动一些手脚（假设该服务器部署于 Windows Server 2003 系统中），让局域网上网安全更有保障！

的新建保留设置框。

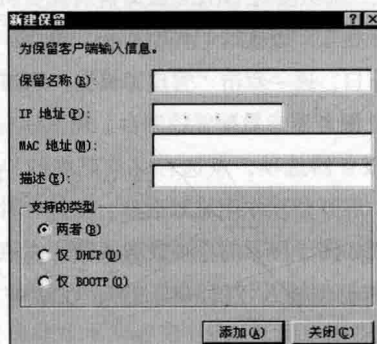


图1 新建保留设置框

保护重要主机安全

局域网中类似服务器这样的重要主机，由于始终在线为其他上网终端系统提供服务，它使用的 IP 地址一般会固定不变。但如果 DHCP 服务器中的地址池参数配置不当，重要主机的 IP 地址有时会出现被强行抢用的安全威胁，这容易造成其不能安全稳定地对外提供在线服务。为了避免这样的安全威胁，我们可以在 DHCP 服务器的配置控制台中，将重要主机使用的 IP 地址保留下来，确保其任何时候都不会被普通上网终端系统随意抢用。

首先以超级用户身份登录进入 DHCP 服务器所在主机系统，逐一点选“开始”、“设置”、“控制面板”命令，进入系统控制面板窗口，依次双击“管理工具”、“DHCP”图标，弹出 DHCP 服务器参数配置控制台。用鼠标右键单击特定 DHCP 服务器选项，点选右键菜单中的“属性”命令，展开指定 DHCP 服务器属性设置对话框。

其次检查重要主机使用的 IP 地址，是否位于 DHCP 服务器的动态地址池中，如果不在其中，那就没有必要建立保留地址。如果看到这个 IP 地址处于动态地址池中时，可以选中重要主机所在的 DHCP 服务器特定作用域，打开它的右键菜单，单击“保留”命令，从弹出的右键菜单中执行“新建保留”命令，切换到如图 1 所示

最后在该设置对话框中，输入好保留名称、保留地址以及重要主机的网卡物理地址，按下“添加”按钮，完成重要主机保留 IP 地址的创建操作。这样，重要主机日后就不需要参与 IP 地址的动态分配了，而新建的保留 IP 地址为重要主机单独使用，以后该主机就不会出现类似 IP 地址被突然抢用的安全威胁了。

值得注意的是，在创建保留 IP 地址时，将欲保留的某个目标 IP 地址，和需要固定 IP 地址的重要主机网卡 Mac 地址捆绑在一起即可。重要主机的网卡 MAC 地址获取，可以在对应主机系统的 MS-DOS 窗口中，通过使用“ipconfig /all”命令来查询。

保护网络运行安全

在一些组网规模较小的工作环境中，网络管理员常常会为终端计算机分配一段连续的静态 IP 地址，同时在上联防火墙或路由器上采用 NAT 技术来实现网络访问目的。但就是这样规模的网络，运行特别不稳定，IP 地址抢用现象频繁发生，这主要就是终端用户在重装系统后，忘记以前使用的 IP 地址，于是随意设置一个，或者将私人笔记本电脑带到单位后，随意为其分配一个 IP 地址，结果自然容易引起 IP 地址抢用现象。发生这

种现象时，一般很难快速找到抢用者，一是网络环境较差，网管员不方便通过专业监控工具寻找被抢用 IP 地址，二是终端用户自己不是很配合。为了保护网络稳定运行，我们可以通过对 DHCP 服务器进行针对性设置，让终端用户抢用地址现象有效避免。

首先为局域网分配特定范围的 IP 地址。例如，如果为单位局域网分配的 IP 地址段为 10.168.1.22-10.168.1.58，为 DHCP 服务器分配的 IP 地址为 10.168.1.26，掩码地址为 255.255.255.0，网关地址为 10.168.1.22。那只要在 DHCP 服务器所在主机系统，依次单击“开始”、“设置”、“控制面板”命令，进入系统控制面板窗口，逐一双击“管理工具”、“DHCP”图标，弹出 DHCP 服务器参数配置控制台。用鼠标右键单击特定 DHCP 服务器选项，点选右键菜单中的“新建作用域”命令，展开创建作用域对话框，点选“常规”选项卡，切换到如图 2 所示的选项设置页面，在该页面起始 IP 地址文本框中输入“10.168.1.22”，在结束 IP 地址文本框中输入“10.168.1.58”。

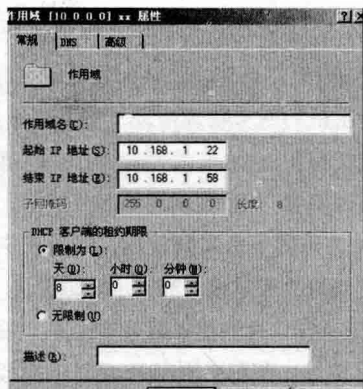


图 2 选项设置页面

接着将租约期限、添加排除这两个参数都设置为默认值，当向导对话框提示是否“配置 DHCP 选项”时，选中“否，我想稍后配置这些选项”，确认后返回 DHCP 服务控制台界面。右击刚刚创建的作用域选项，单击右键菜单中的“配置选项”命令，进入配置选项对话框，点选“高级”选项卡，打开高级选项设置页面。在这里，选中“003 路由器”选项，通过该选项将单位局域网的网关地址 10.168.1.22 自动分配给上网终端系统，选中“006 DNS 服务器”选项，通过该选项将局域网的 DNS 服务器地址动态分配给终端计算机。之后在特定作用域名称上，单击鼠标右键，执行右键菜单中的“激活”命令，让 DHCP 服务器按照既定配置要求，立

即为终端计算机提供网络服务。

为了让终端计算机正确从 DHCP 服务器那里获取上网地址，还要对其网络连接进行设置，让其自动获得 IP 地址。在进行该操作时，逐一单击“开始”、“设置”、“网络连接”命令，右击本地连接图标，单击右键菜单中的“属性”命令，展开本地连接属性设置窗口，选中 TCP/IP 协议选项，按下“属性”按钮，进入如图 3 所示属性对话框，选中“自动获得 IP 地址”选项，最后单击“确定”按钮保存设置操作。这样，在这个小规模局域网中成功启用 DHCP 服务器后，IP 地址抢用现象基本上就能得到控制，那么网络运行也就相对安全了。

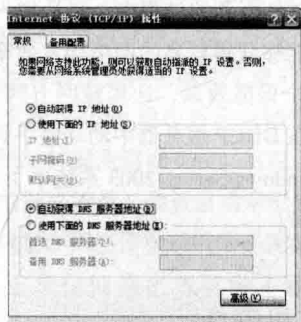


图 3 属性对话框

保护终端接入安全

局域网中的很多终端计算机，或多或少地会感染些病毒，如果让其从 DHCP 服务器那里自由申请上网地址接入网络的话，那么整个局域网很可能都被感染网络病毒，显然这会给网络稳定运行带来很大安全威胁。如何才能让安全、可信的终端计算机从 DHCP 服务器那里获取上网地址，而不可信的终端计算机禁止从 DHCP 服务器那里获得上网地址呢？很简单！只要在 DHCP 服务器中动动以下手脚，让其依照事先设置的用户 ID，来判断待接入网络的用户是否为合法、可信用户。

首先进入 DHCP 服务器所在主机系统，逐一点选“开始”、“程序”、“管理工具”、“DHCP”选项，展开 DHCP 控制台窗口，右击 DHCP 服务器主机名称，从右键菜单中选择“定义用户类别”命令，切换到新建类别向导对话框。依照操作提示，先设置一个合法可信 DHCP 用户的 ID 为“1234”，在 ASCII 列表下定义好由终端计算机系统提供的 ID，局域网 DHCP 服务器日后会借助该 ID 内容来匹配类 ID，这里假定输入的 ASCII 字符也为“1234”，确认后结束合法可信 DHCP 用户 ID

的定义操作。

之后要为该合法可信用户 ID 配置正确的上网参数。在进行该操作时，先从 DHCP 服务器控制台界面中选择合适的“作用域选项”，同时用鼠标右击该选项，从弹出的右键菜单中执行“配置选项”命令，在其后界面中点击“高级”选项卡，展开如图 4 所示的选项设置页面，在这里为合法可信的终端计算机用户正确定义好路由地址、DNS 参数、IP 地址租约期限以及其他上网参数等，保证合法可信的终端计算机日后能从 DHCP 服务器那里申请得到各种需要的上网地址。

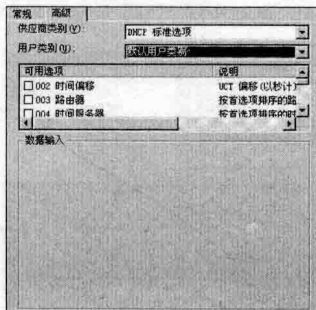


图 4 选项设置页面

接下来需将安全可信的 DHCP 客户端系统的 DHCP 类 ID 串定义为“1234”，日后 DHCP 服务器会该内容进行自动校验，要是校验通过，DHCP 服务器就会认为该客户端系统是安全可信的，那么它就能获得一切正确的上网地址，来顺利地接入到局域网中。

反之，如果校验不成功的话，那么 DHCP 服务器就会拒绝为之提供各种上网参数动态分配服务，这样非安全可信的终端计算机自然就不能随意接入到局域网环境中了。

在定义 DHCP 客户端系统的 DHCP 类 ID 内容时，逐一单击“开始”、“运行”命令，弹出系统运行对话框，输入“cmd”命令，单击回车键后，打开 DOS 命令行工作窗口；在该窗口下，输入命令“ipconfig /setclassid Local Connection 1234”，就能将终端计算机系统本地连接的 DHCP 类 ID 内容指定为“1234”了。如果合法用户的计算机系统中只包含一个网络连接，那么还能使用字符串命令“ipconfig /setclassid * 1234”，将终端计算机系统网络连接的 DHCP 类 ID 内容定义为“1234”了。

下面将终端计算机系统的上网地址修改成动态获取。依次单击“开始”、“设置”、“网络连接”命令，进入网络连接列表窗口，打开“本地连接”图标的右键菜单，单击“属性”命令，切换到本地连接的属性设置对

话框，点选“常规”选项卡，在常规选项设置页面中，单击“Internet 协议 (TCP/IP)”选项，按下“属性”按钮，进入 TCP/IP 协议属性对话框，同时选中“自动获得 IP 地址”、“自动获得 DNS 服务器地址”等选项，确认后退出设置对话框。

如此一来，DHCP 类 ID 内容为“1234”的终端计算机系统，日后要进行网络连接时，会先向局域网传输广播信息申请上网参数，DHCP 服务器收到相关请求后，自动校验它的 ID 内容，校验成功后会将正确的上网地址自动反馈给终端计算机系统，包括路由地址、DNS 参数、IP 地址租约期限以及其他上网参数等，这时局域网的接入就会比平时安全很多。

预防 ARP 欺骗攻击

大家知道，在局域网中通过 ARP 网络协议的漏洞，恶意用户能对整个网络的安全造成巨大威胁，那么怎样才能有效预防局域网遭遇 ARP 欺骗攻击呢？很多用户都会选择对终端计算机的 IP 地址和 MAC 地址进行捆绑，但逐一在每台终端计算机中执行地址绑定操作，不利于提高操作效率。其实，我们可以通过在 DHCP 服务器中进行合适配置，来保证局域网中的终端计算机，不会遭遇 ARP 欺骗攻击。

首先获取终端计算机的上网参数。正常情况下，一个局域网的初始组网资料中，应该包含所有终端计算机 IP 地址和 MAC 地址的关系表，要是手头没有现成档案资料时，可以进入终端计算机的系统运行对话框，输入“cmd”命令，展开 DOS 命令行窗口，在该窗口命令提示符下，执行字符串命令“ipconfig /all”，返回如图 5 所示的结果信息，从中就能获取终端计算机的 IP 地址和 MAC 地址。

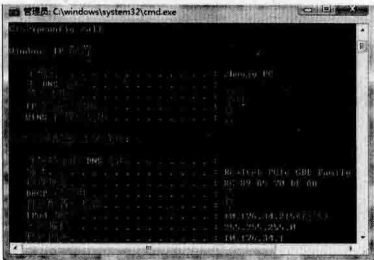


图 5 结果信息

其次进行地址绑定操作。先以超级用户身份进入 DHCP 服务器所在主机系统，依次单击“开始”、“设置”、“控制面板”命令，展开系统控制面板窗口，双击“管

理工具”、“DHCP”图标,弹出 DHCP 控制台界面。将鼠标定位到特定作用域节点下面的“保留”选项上,打开它的右键菜单,点选“新建保留”命令,在新建对话框“保留名称”位置处,输入好对应 IP 地址的保留名称,在“IP 地址”栏中设置好特定计算机使用的 IP 地址,

在“MAC 地址”位置处输入对应计算机系统的网卡物理地址,同时将“支持类型”参数调整为“两者”选项,确认后完成特定计算机的地址绑定操作。同样地,将其他终端计算机的 IP 地址和 MAC 地址也绑定起来,这样就能成功预防 ARP 欺骗攻击现象了。

让服务器网络更安全

江苏 弯弯

让 DNS 服务更安全

首先,严格限制远程访问权限。要是普通用户可以自由远程访问并修改 DNS 服务器中的重要内容,那么 DNS 服务器的工作安全性将不能得到有效保障。所以,严格限制 DNS 服务器的远程访问权限,保证其不会被非法用户远程攻击,是相当有必要的。只要用鼠标右击系统桌面上的“计算机”图标,从右键菜单中点选“管理”命令,依次展开计算机管理界面中的“系统工具”、“本地用户和组”、“用户”分支,双击指定分支下的来宾账号,在对应账号属性设置框中,勾选“账号已停用”选项,确认后退出设置对话框。接着依次点击“开始”、“运行”命令,弹出系统运行文本框,在其中执行“gpedit.msc”命令,开启系统组策略编辑器运行状态;找到“本地计算机策略”、“计算机配置”、“Windows 设置”、“安全设置”、“本地策略”、“用户权限分配”分支选项,用鼠标双击“从网络访问此计算机”组策略选项,弹出如图 1 所示的组策略属性对话框,删除所有陌生用户账号,再将我们认为合法可信的用户账号添加导入进来,最后重启一下 DNS 服务器所在主机系统即可。

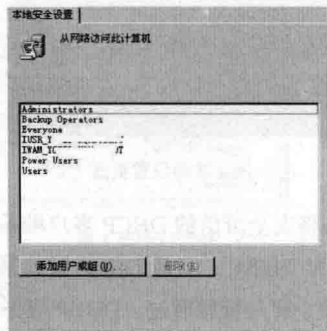


图 1 组策略属性对话框

其次,多措并举预防缓存攻击。一是禁用防止缓存污染功能。为了防止自己的 DNS 服务器缓存被黑客攻击,Windows Server 2003 系统在默认状态下支持 DNS 服务器启用“防止缓存污染”功能,来保护缓存内容不被虚假信息“污染”;要是发现该功能还没有被启用时,我们只要进入 DNS 服务器属性配置对话框,点击“高级”标签,在对应标签页面中选中“防止缓存污染”选项,再将 DNS 服务器所在主机系统重新启动一下即可。二是禁用 DNS 缓存功能。可以有两种方法,一种方法是临时性的,只要依次单击“开始”、“运行”命令,弹出系统运行对话框,在其中执行“cmd”命令,进入系统的 DOS 命令行窗口,在该窗口中执行“net stop dnscache”命令, DNS 缓存功能就会被临时禁用了,不过系统重新启动之后,该功能又会立即生效了。另外一种方法是永久性的,只要按照上面介绍的方法,停用“DNS Client”服务工作状态即可。当然,一旦停用了 DNS 解析器缓存功能后,客户机的总体性能会降低,同时 DNS 请求查询的网络通信量会增加,这可能会给

上网浏览的速度造成一定的影响。三是将 DNS 服务器的 TTL 值修改得稍微小一些。依次单击“开始”、“运行”命令，在弹出的系统运行对话框中，执行“regedit”命令，弹出注册表编辑窗口，在该编辑窗口的左侧列表中，依次展开“HKEY_LOCAL_MACHINE\System\CurrentControlSet\Services\Tcpip\Parameters”注册表分支（如图 2 所示），从目标分支下面找到“DefaultTTL”键值（如果没有找到可以自行创建），用鼠标双击该键值，在弹出的编辑对话框中我们可以将 TTL 值修改为“64”或“32”，再单击“确定”按钮，并刷新系统注册表，这样 TTL 数值就变小了！



图 2 注册表分支

第三，谨防非法访问配置信息。要是单位网络中部署了独立的 DNS 服务器，那么在缺省状态下，服务器配置信息会存储在系统 DNS 文件夹中，还有一些配置会存储在注册表相关分支下。如果黑客自由访问这些配置信息，同时对其随意篡改的话，DNS 服务安全性将不能得到保证。为了防止黑客非法访问这些配置，可以先登录 DNS 服务器所在主机系统，进入 Windows 资源管理器窗口，依次双击“WinNT”、“System32”、“DNS”文件夹图标，打开“DNS”文件夹的右键菜单，点击“安全”命令，切换到对应文件夹安全设置页面，在这里只为合法可信用户分配编辑调整权限，将其他人的操作权限全部取消即可。之后进入系统注册表编辑界面，将鼠标定位到注册表分支“HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Services\DNS”上，打开目标分支选项的右键菜单，单击“权限”命令，展开如图 3 所示的权限调整对话框，在这里只保留合法可信用户账号，同时为对应账号分配修改权限，这样就能防止用户通过注册表修改 DNS 配置了。



图 3 权限调整对话框

第四，及时追踪潜在安全隐患。要是能将 DNS 服务器的运行状态信息自动追踪记录下来，日后有针对性地查询、分析其中内容，就可以在第一时间追踪到 DNS 服务器中存在的潜在安全隐患。在缺省状态下，DNS 服务器的日志功能并没有启动运行，管理员只要在 DNS 服务器所在主机系统中，进行如下设置操作，就能成功启用这项功能：首先以超级用户身份登录进入 DNS 服务器所在主机系统，依次单击“开始”、“程序”、“管理工具”、“DNS”命令，切换到 DNS 控制台窗口，用鼠标选中 DNS 服务器主机名称，同时用鼠标右击之，单击右键菜单中的“属性”命令，切换到 DNS 服务器属性设置对话框。接着点选“事件日志”选项卡，展开如图 4 所示的选项设置页面，在这里选中需要跟踪记忆的状态信息，确认后 DNS 服务器日后会将所有状态信息自动存储在系统日志文件中。当需要查询分析日志内容时，只要进入 DNS 服务器的事件查看器窗口，从中就能查询到 DNS 各方面的状态信息，例如 DNS 查询、应答、发送、接收等方面的状态信息等，依照这些信息，管理员基本就能判断出 DNS 服务器的安全状况了。

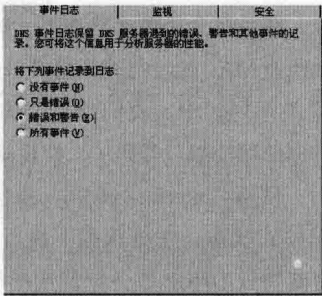


图 4 选项设置页面

让 DHCP 服务更安全

首先强制进行域认证。为了防止授权 DHCP 服务器

受到非授权 DHCP 服务器干扰，系统管理员可以通过域认证方式，确保终端计算机优先从授权 DHCP 服务器那里获得上网参数。在将合法、授权 DHCP 服务器添加到局域网指定域时，可以进行如下设置操作：首先以超级用户身份登录特定域控制器所在主机系统，依次单击“开始”、“程序”、“管理工具”、“DHCP”命令，弹出 DHCP 服务器控制台窗口。在该界面左侧显示区域，用鼠标右击本地主机名称，点击“添加服务器”命令，弹出如图 5 所示的添加服务器对话框，按下“浏览”按钮，从其后续界面中选择并导入合法授权的 DHCP 服务器所在主机名称，也能在“此服务器”位置处直接输入 DHCP 服务器主机地址，确认后保存设置操作。这样，特定域中的网络终端主机日后上网访问时，就会优先从授权的 DHCP 服务器那里获取有效的上网地址。尽管这种方法保护效果很好，不过在组网规模不大的上网环境中，基本不会用到域工作模式，那么这种方法也就没有实现的基础。其实，现在局域网使用的交换机都支持网络管理功能，我们可以在交换机后台系统中，封杀非授权 DHCP 服务器使用的交换端口，让其无法干扰合法 DHCP 服务器的正常工作。当然，这种方法需要想办法找到非授权 DHCP 服务器使用的端口号码。例如，某台非授权 DHCP 服务器所在主机的 IP 地址为 10.176.34.168，它与一台 H3C 系列的交换机相连，要找到它使用的交换端口号码时，可以先在网络中的一台终端主机系统中，打开 DOS 命令行窗口，输入“ping -a 10.176.34.168”命令，获取它的计算机主机名称。接着使用 Arp 命令，查询对应主机使用的网卡 MAC 地址，也能到授权 DHCP 服务器系统中，查看缓存池中特定 IP 对应的 MAC 地址。弄清楚了 MAC 地址后，登录交换机后台系统，在系统全局模式状态下，执行“display mac”命令显示所有 MAC 地址与交换机端口的对应关系。从显示的对应关系列表中，我们就能准确定位到非授权 DHCP 服务器使用的端口号码了，假设该端口号码为“e0/36”。最后，使用“interface e0/36”命令，进入对应交换端口视图模式状态，在该状态下执行“shutdown”命令，就能将非授权 DHCP 服务器使用的端口封杀掉，这样授权 DHCP 服务器就能安全、稳定地工作了。

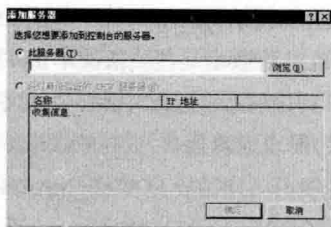


图 5 添加服务器对话框

其次，集中进行绑地址。在局域网中 IP 地址被盗用的现象非常频繁，这种现象容易引起网络运行不安全。为了避免 IP 地址被盗用，管理员不妨在 DHCP 服务器中，对特定网络终端主机的 IP 地址和 MAC 地址进行集中捆绑。首先查询终端地址。打开终端系统的运行对话框，输入“cmd”命令并回车，展开 DOS 命令行窗口，在该窗口命令提示符状态下执行“ipconfig /all”命令，获取计算机的 IP 地址和 MAC 地址。其次进行地址绑定。在 DHCP 服务器中进行地址绑定操作时，可以先进入 DHCP 服务器所在主机系统，在系统控制面板中逐一双击“管理工具”、“DHCP”图标，切换到 DHCP 控制台窗口，将鼠标定位到特定作用域节点下面的“保留”选项上，打开它的快捷菜单，点击“新建保留”命令，在其后续界面的“保留名称”栏中（如图 6 所示），输入好特定 IP 地址的保留名称，在“IP 地址”栏中设置好特定计算机使用的 IP 地址，在“MAC 地址”栏中输入对应计算机的网卡物理地址，同时将“支持类型”参数设置为“两者”选项，确认后完成特定计算机的地址绑定操作。同样地，将其他终端计算机的 IP 和 MAC 地址也绑定起来。日后，局域网用户即使抢用了重要网络终端的 IP 地址，他们也无法通过该地址连接到局域网中，那么整个网络运行自然就安全了。

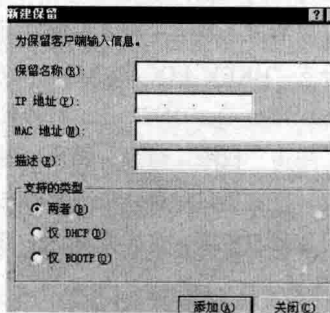


图 6 输入保留名称

第三，开启 DHCP 监听功能。在局域网交换机支持 DHCP 监听功能的情况下，可以使用该功能控制普通用户只允许对外发送 DHCP 数据包，同时自动丢弃来自该用户端口的其他 DHCP 数据包，从而达到预防非法

DHCP 服务器干扰授权 DHCP 服务器目的。以 H3C 系列交换机为例，要开启它的 DHCP 监听功能时，先以超级用户身份登录交换机后台系统，使用“system-view”命令，切换到全局视图模式，输入“dhcp-snooping”命令，开启全局 DHCP 监听功能。这时，交换机就能对单位网络中存在的所有 DHCP 数据报文进行自动侦听，并限制非信任端口只能对外发送 DHCP 数据包，而不能发送其他 DHCP 数据包，日后即使有未授权 DHCP 服务器偷偷连接到单位网络中，该功能将会自动对它进行屏蔽，确保局域网中的所有终端可以稳定地从授权的 DHCP 服务器那里申请得到 IP 地址。要想让交换机特定端口可以正常接收各类 DHCP 数据报文，同时对它们进行转发时，还可以将指定交换端口配置成可信任端口。例如，想配置交换机上的 G0/1/16 端口成为合法交换端口时，只要先进入后台系统的全局视图模式，输入“interface G0/1/16”命令，进入如图 7 所示的特定端口视图状态，再执行“dhcp-snooping trust”命令即可。日后，目标交换端口就可以任意接收或转发所有 DHCP 数据包了。一般来说，当单位网络中的 DHCP 中继设备与交换机保持直接连接状态时，只要互连端口处于 Trunk 模式，那么管理员就应该将该交换端口配置成合法端口。

```

* no decompiling or reverse-engineering shall be allowed
*****

login authentication

password:
VCK2_U_P8512>su
Password:
low user privilege is 3 level, and only those commands
equal to or less than this level can be used.
? privilege note: 0-VISIT, 1-MONITOR, 2-SYSTEM, 3-MANAGE
VCK2_U_P8512>sys
System View: return to User View with Ctrl-Z.
VCK2_U_P8512>inter g1/1/16

% Wrong parameter found at '' position.
VCK2_U_P8512>inter g0/1/16
VCK2_U_P8512>

```

图 7 特定端口视图状态

让 Web 服务更安全

首先限制 Web 访问权限。正常情况下，非法用户都是先窃取 Web 站点主目录访问权限，来破坏 WEB 服务运行安全的。为了避免这种现象发生，管理员有必要进入 Web 站点属性设置框，严格限制站点主目录访问权限，具体操作步骤为：依次单击“开始”、“设置”、“控制面板”，双击“管理工具”、“Internet 服务管理器”等图标，展开 IIS 控制台界面。右击 Web 站点名称，点选

右键菜单中的“属性”命令，选择指定站点属性设置框中的“目录安全性”标签，进入如图 8 所示的标签页面，按下“匿名访问和身份验证控制”旁的“编辑”按钮，在其后页面中导入安全可信的用户账号，并将其他用户账号依次删除掉。之后切换到“主目录”标签页面，在“应用程序设置”位置处单击“配置”按钮，选中与 ASPX 相关的功能选项。进入系统资源管理器窗口，从中找到 WEB 站点所用根目录，打开它的右键菜单，选择“属性”命令，进入“安全”标签页面，逐一删除这里的所有陌生用户账号，将合法可信的用户账号导入进来，并为它们设置好合适的访问权限，确认后保存设置操作。

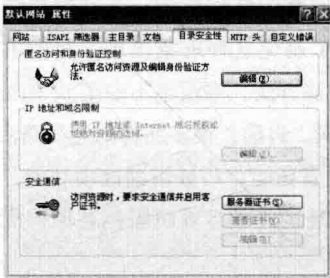


图 8 标签页面

其次，拦截 SQL 注入攻击。所有的 SQL 注入都是从访问者输入开始的，如果 Web 站点对所有用户输入进行了判定和过滤，那么就能有效防止 SQL 注入攻击了。如果 Web 站点是用户自行编写代码开发设计的，那就必须要对类似 request.form、request.querystring 这些 get 或 post 请求中的参数信息进行过滤和修改，保证要过滤掉 #、%、select 这样的非法字符。倘若 Web 站点是通过动易等免费代码开发设计的，它们一般都有预防 SQL 注入功能，只要手工启动运行这类功能，就能有效拦截 SQL 注入攻击了。

第三，加强 Web 身份验证。进入 Web 站点的目录安全选项设置页面，单击“安全通信”处的“编辑”按钮，将“要求安全通道（SSL）”、“要求 128 位加密”等选项依次选中，在“身份验证和访问控制”位置处按“编辑”按钮，将“启用匿名访问”、“集成 Windows 身份验证”这些选项的选中状态全部取消，再将“基本身份验证”选中即可。

❖ 巧妙谢绝危险访问

▼ 江苏 周勇生

谢绝使用无线网络

如果单位的无线网络允许不安全 IP 地址使用, 既会降低无线网络的传输性能, 又会给单位网络带来安全威胁。为了避免这种现象出现, 我们不妨利用网卡 MAC 地址过滤方法, 来谢绝不安全 IP 地址偷偷使用单位无线局域网。目前, 很多品牌的无线路由设备都具有 MAC 地址过滤功能, 巧妙借助这项功能, 能有效地将不安全 IP 地址的终端计算机阻挡在单位无线网络大门之外。

众所周知, MAC 地址其实是一种硬件地址, 它由 12 位 16 进制数组成, 一共长 48 比特, 专门用来指定网络设备位置的, 前面 24 比特主要用来标识厂商的, 后面 24 比特由厂商自行分派。所有上网的设备一般都有一个全球唯一静态的 MAC 地址, 将无线网络中安全可信计算机的 MAC 地址, 手工导入到无线路由器内置的 MAC 地址过滤表中, 日后只有拥有这些 MAC 地址的终端计算机, 才会被无线路由器识别为安全可信计算机, 从而有资格接入单位无线网络中进行上网访问, 其他计算机都会被识别为不安全地址, 它们是无法上网访问的。

在谢绝不安全 IP 地址使用单位无线网络时, 首先以管理员权限登录进入无线路由器后台系统, 将鼠标定位到左侧列表中的“安全设置”、“防火墙设置”节点上, 在指定节点的右侧设置区域中, 将“开启 MAC 地址过滤”勾选起来, 并且在“缺省过滤规则”设置项处, 选中“仅允许已设 MAC 地址列表中已启用的 MAC 地址访问 Internet”选项, 按下“保存”按钮退出设置保存区域。

之后将鼠标返回到无线路由器后台系统页面的“安全设置”、“MAC 地址过滤”节点上, 在指定节点下单击“添加新条目”按钮, 弹出新条目添加设置框, 正确输入安全可信计算机系统的网卡 MAC 地址, 按下“保存”按钮退出。按照相同的操作方法, 依次将单位无线网络中其他安全 IP 地址对应的 MAC 逐一导入进来, 最后也要记得执行保存操作。

完成上述设置任务后, 日后只有安全的 IP 地址才能使用无线路由器, 进行无线网络访问操作, 而不安全 IP 地址在尝试进行无线连接时, 无线路由器因为无法正确识别它们的 MAC 地址, 将会认为它们是不安全连接, 并将他们拒之门外。

谢绝访问重要网站

一些重要的网站, 每天的访问量可能很高, 如果在某个时刻若干个不安全 IP 地址, 同时访问对应网站上的内容, 将会给网站的运行稳定性和安全性带来很大的挑战。为了保护重要网站的安全, 想办法谢绝那些不安全 IP 地址的访问, 是相当有必要的。

正常来说, 那些不安全 IP 地址进行 Web 访问时, 都会在服务器的系统日志中留下痕迹, 通过查看日志内容, 找出这些不安全 IP 地址究竟来源于什么位置。例如, 笔者曾经发现某个网站页面, 在遭遇短时间内高强度访问后, 通过查看相关日志信息, 看到不安全地址大多来源于 61.157.100.*、60.155.82.* 这两个网段。考虑到这些不安全 IP 地址在 Web 访问时, 都需要经过域名解析环节, 笔者决定取消这些网段的域名解析服务, 这样它们的 Web 访问请求就到不了指定的重要站点服务器。

在 Apache 服务器环境下, 通过编辑 .htaccess 文件, 就能很轻易地谢绝不安全 IP 地址访问重要网站。从特定网站的根目录下面找到 .htaccess 文件, 借助文本编辑器打开该文件, 在其中添加如下代码即可:

```
<IfModule mod_rewrite.c>
RewriteEngine On
##Block ip
RewriteCond %{http:X-Forwarded-For}&%{REMOTE_ADDR} (61.157.100|60.155.82)[NC]
RewriteRule (.*)-[F]
</IfModule>
```

经过实际测试，来源于 61.157.100.*、60.155.82.* 这两个网段的不安全 IP 地址，果然被 Web 服务器拒绝访问了。

当然，要是大家不知道哪些 IP 地址是不安全的，也可以尝试到特定站点的日志文件中去寻找，不安全 IP 地址进行 Web 访问时，往往都有十分明显的特征，例如说在特定的时间内进行访问，仅对站点下的某一个特定页面内容进行访问并多次来访，使用的终端系统分辨率是一样的，上网的浏览器版本也是一样的，只要不安全 IP 地址具有这几个特征，建议大家谢绝它们的访问。

谢绝随意更改地址

单位局域网环境下，有些不安全 IP 地址为了躲避上网限制，常常会私自更改地址，这容易造成整个局域网的管理混乱。有鉴于此，我们可以使用“easy 网管”这款外力工具，来限制不安全 IP 地址用户随意更改上网地址。

在进行该操作时，大家不妨先从 Internet 网络中下载获得最新版本的“easy 网管”程序，之后在单位网管计算机中安装好该工具的服务端程序，在局域网其他普通计算机中安装好该工具的客户端程序。

下面在网管计算机中启动运行“easy 网管”程序，弹出如图 1 所示的主操作界面，在该界面中大家就可以直观看到单位网络中所有终端计算机的网络连接状态（当然所有终端计算机都需要事先安装好“easy 网管”的客户端程序）。“easy 网管”程序在缺省状态下，是禁止所有 IP 地址用户随意更改上网地址的，要是他们自行调整了自己计算机的 IP 地址时，该管理工具将自动强制特定计算机断开网络连接，如果希望重新上网访问，一定要请网络管理员帮忙才能解决问题。这种管理措施控制效果还是相当好的，任何不安全 IP 地址用户，甚至是安全 IP 地址用户，都无权利修改上网 IP 地址；只是该方法操作起来有点麻烦，需要在单位局域网的服务器和普通计算机中依次安装好相关控制程序才行。



图 1 主操作界面

谢绝使用有线网络

要想谢绝不安全 IP 地址使用有线网络，可以使用可管理交换机的端口绑定功能，仅允许那些管理员认为合法的终端计算机访问网络，其他终端用户即使抢用了别人的安全 IP 地址，也不会引起网络运行混乱。

例如，单位网络中有一台 Web 服务器，使用了“10.172.11.20”的 IP 地址，为了防止不安全 IP 地址用户抢用该地址，造成 Web 服务器不能正常访问，管理员不妨在单位网络的核心三层交换机后台系统，将 Web 服务器的“10.172.11.20”地址与网卡 MAC 地址相互绑定在一起。这时，即使有不安全用户抢用了该 IP 地址，他们也不能使用该地址接入单位局域网，那么单位网络的运行就不会轻易受到干扰。下面就是详细的操作操作步骤：

首先获取 Web 服务器的网卡 MAC 地址，以管理员权限登录进入 Web 服务器所在主机系统，逐一点选“开始”、“运行”命令，展开系统运行对话框，输入“cmd”命令进入 MS-DOS 工作窗口。在该窗口命令提示符下，输入“ipconfig /all”命令，从返回的如图 2 所示结果信息中，不难看出 Web 服务器所在主机的网卡 MAC 地址为“d4bc.d98e.a847”。



图 2 结果信息

其次执行地址绑定操作。登录单位局域网交换机后台系统，进入系统全局视图模式，执行“address-bind 10.172.11.20 d4bc.d98e.a847”命令，就能将 Web 服务器 IP 与 MAC 地址绑定在一起了。之后使用“arp 10.172.11.20 d4bc.d98e.a847 arpa gigabitEthernet 1/3”命令，将 Web 服务器地址绑定到其所连的交换机光口上。如此一来，单位网络中的不安全 IP 地址，将无线通过交换机使用有线网络，即使他们抢用了 Web 服务器 IP 地址，也不会造成 Web 服务器上网不稳定现象，这是因为其他不安全 IP 地址用户无法使用“10.172.11.20”这个 IP 地址进行网络接入操作。

此外，如果单位网络是通过路由器来组网的，管理员也可以使用路由器自带的“IP 与 MAC 绑定”功能，

实现不安全地址的谢绝访问操作。例如,在通过 TP-LINK R480T 宽带路由器组网环境中,管理员可以使用 IE 浏览器窗口,远程打开路由器后台系统管理页面,将鼠标定位到“IP 与 MAC 绑定”、“静态 ARP 绑定设置”节点上,在对应节点设置区域,将“ARP 绑定”修改为“启用”,单击“保存”按钮后退出设置页面,再按下“增加单个条目”按钮,将先前获取到的 Web 服务器 IP 地址与 MAC 地址绑定起来就 OK 了。

谢绝进行 Ping 攻击

大家知道,通过 Windows 系统内置的 Ping 命令,能够测试出特定计算机的在线状态。但是,经常有一些恶意用户会通过该命令,频繁地向单位网络中的服务器发送 Ping 测试包,例如,在 MS-DOS 命令行窗口中,使用“ping-l 65500-t xx.xx.xx.xx”命令(这里的“xx.xx.xx.xx”为单位网络中的服务器主机 IP 地址),就能向特定服务器主机发送大量的 ping 测试包数据;如果不安全 IP 地址用户在局域网的多台终端系统中同时使用“ping-l 65500 -t xx.xx.xx.xx”命令,那么特定服务器主机的宝贵系统资源将会很快被消耗殆尽,最终会造成服务器系统发生瘫痪现象。

要想防止不安全 IP 地址的 Ping 命令攻击,管理员

可以在单位网络特定服务器主机中使用类似天网防火墙这样的安全保护工具,同时打开对应防火墙的安全配置窗口,勾选“不允许别人用 Ping 命令探测本机”功能选项即可。当然,如果管理员身边暂时没有专业防火墙工具时,也能通过 Windows 服务器系统内置的防火墙程序,谢绝不安全 IP 地址用户发起的 Ping 命令攻击。例如,在 Windows Server 2008 服务器系统环境下,巧妙使用系统内置防火墙,就能轻松谢绝不安全 IP 地址用户进行 Ping 攻击,下面就是具体的操作步骤:

首先逐一单击“开始”、“所有程序”、“管理工具”命令,用鼠标双击管理工具列表中的“高级安全 Windows 防火墙”图标,打开服务器系统高级安全 Windows 防火墙程序界面。点击左侧显示区域中的“入站规则”选项,选择“新规则”标签,展开新建入站规则向导设置框。按照向导设置框的提示,先将新建防火墙的规则类型设置为“自定义”,配置好与该防火墙规则保持匹配的应用程序详细路径,选中“所有程序”项目,将防火墙规则协议类型设置为“ICMPv4”,再从端口下拉列表以及远程端口下拉列表选中“所有端口”,同时将防火墙规则选择为匹配所有不安全的 IP 地址,最后勾选“阻止连接”选项,确认后退出设置对话框。这样一来,服务器系统就会自动谢绝所有不安全 IP 地址用户发动的 Ping 命令攻击。

提高 Linux 安全技巧

河南 刘进京

在 Windows 中,利用系统提供的 Update 功能,可以执行系统的更新操作,也就是为系统打上各种补丁。与之对应,不同的 Linux 系统都有各自的更新程序,利用其可以自动搜索更新包并完成安装操作,将系统中的所有软件包升级到最新版本。登录密码可谓系统的第一道也是最重要的防线,如果您的 Linux 系统使用的是默认的空密码,而且还开启了 Telnet、SSH 等服务的话,就等于为黑客入侵开启了大门。因此,当系统安装完毕后,必须立即更改 Root 等账户的密码,可以使用

Passwors 命令来修改密码,其使用格式为“password 账户名”。当然,只有超级用户才可以修改不同账户的密码。如果在命令行中执行“password”命令,修改的是 Root 账户的密码,而且密码输入时不回显的。虽然使用图形界面也可以修改密码,不过使用 Linux 一定要养成使用终端的习惯。对口令的保护还涉及到对“/etc/passwd”和“/etc/shadow”文件的保护,只有系统管理员才可以访问这两个文件。

系统的所有活动信息都会记录在日志中,如果黑客入侵了系统,其行踪自然逃不出日志的法眼。Linux 的

日志文件一般保存在“/var/log”目录中,在该目录下会发现名称后面带有数字的文件,这些文件是在日志文件被循环的时候创建的,因为是循环使用日志,其体积不会太大。但是,当黑客攻击系统后,往往会修改,删除日志来逃避检测。所以一定要限制“/var/log”目录的访问权限,禁止一般权限的用户查看,修改日志内容。大部分日志使用的是纯文本模式,任何文本编辑器都可以查看其内容。当然,也可以使用系统自带的工具,例如在 Redhat Linux 中运行其内置的 Logviewer 程序,可以以图形化界面显示日志信息,其界面更加细致简洁,看起来很方便。当然,也可以使用 Logcheck 这款专业工具来分析日志,该工具可以自动检查和安全相关的入侵事件以及非正常活动记录,可以有效分析各种 Linux 日志文件,例如“/var/log/message”、“/var/log/secure”、“/var/log/maillog”等。

当黑客入侵系统后,往往会和本机建立网络连接,或者在其中安置后门程序,来长期控制系统。在 Linux 中可以使用大家很熟悉的“netstat a”命令,来查看本机端口使用信息。在网络连接列表中如果发现异常的端口连接情况,就必须对系统进行安全检查了。常言道,有备则无患。当黑客入侵后,一旦将重要文件删除,就会给您造成很大的损失。因此,对重要的文件和目录进行备份,是极为重要的。使用系统自带的“tar”命令,就可以完成备份操作,其使用格式为“tar [选项] 文件或目录”,其中的选项分为主选项和辅选项,主选项是必须的,告诉 tar 命令执行什么动作,辅选项是可选的,例如选项“c”表示创建新的文档文件,“r”表示把要存档的文件追加到档案文件尾部,例如当备份好文件后,发现有些文件忘记备份了,可以利用该选项,将这些文件追加到备份文件中。“t”参数可以列出档案内容,“u”参数要用来更新档案文件,即使用新增的文件覆盖原备份文件,如果在档案文件中没有更新内容则执行追加操作。“f”参数表示使用档案文件,“x”参数表示释放文件。

例如,需要备份当前路径下的“data”目录,可以执行“tar -cf shuju.tar data”,将其内容被分到“shuju.tar”文件中。以后需要恢复数据时,执行“tar xvf shuju.tar”即可。对于系统中的一些重要目录,建议经常进行备份操作。例如在“/etc/passwd”目录中存储所有用户的信息,包括密码、登录的 Shell 等。在“/etc/fstab”目录中保存文件系统配置信息,在“/etc/inittab”目录中包含配置 Init 在不同运行级别下启动系统参数,在“/etc/hosts”目录中包含域名解析信息,在“/etc/inetd.conf”

目录中包含远程控制信息,在“/etc/printcap”目录中包含打印机通信配置信息,在“/etc/XF86Config”目录中包含 Xfree86 的初始配置信息等,对于上述目录,应该定期进行备份。其实,在“/etc”目录下有很多配置文件都需要及时进行备份的。

当黑客入侵系统后,往往会在其中创建非法账户,来对系统进行深入控制。因此,对用户列表经常进行检查,及时发现并删除陌生的可疑账户,是不可忽视的安全问题。执行“cat /etc/passwd”命令,就可以查看账户列表信息。使用“userdel f”命令,可以删除指定的账户。例如执行“userdel f hack”命令,可以将 hack 账户删除,同时将其关联的目录和文件一并清除。为了提高安全性,需要在 Linux 中使用杀软和防火墙软件。这类安全软件有很多,例如 ClamAV、Mcafee、Avast、Avira、AVG、F-PROT 等。对于防火墙软件来说,可以使用 KDE 自带的防火墙,虽然没有专业版防火墙功能强悍,不过对于一般用户可以满足需求。如果您没有使用 KDE 桌面环境,可以使用系统自带的 IPTables (内核包过滤管理工具),同样可以起到防火墙的作用。其过滤流程的前提是包过滤规则必须被包过滤设备端口存储起来,当包到达端口时,对包的报头进行语法分析,大多数包过滤只检查 IP、TCP、UDP 报头中的字段信息。包过滤规则以特殊的方式存储,应用于包的规则的顺序与包过滤器规则存储顺序必须相同。若一条规则阻止包传输或接收,则此包便不被允许。若一条规则允许包传输或接收,则此包便可以继续处理。若包不满足任何一条规则,则此包便被阻止。

IPTables 的用法是“iptables [-t table]CMD[chain][rule-matcher][-j target]”,其中的“table”是表明,为 filter、nat 和 mangle,包过滤只使用 filter 表,这是默认项目。其中的“CMD”是操作命令,包括添加、删除、更新等。“chain”为链名,对于包过滤防火墙可操作 filter 表中的 INPUT 链、OUTPUT 链和 FORWARD 链,也可以自定义链。

“Rule-matcher”参数是规则匹配器,用来指定各种规则匹配,例如 IP、PORT、包类型等。“Target”为目标动作,当规则匹配一个包时,真正要执行的任务用目标表示,最常用的内置目标为 ACCEPT 和 DROP,当然,也可以使用扩展的目标。看起来包过滤规则很复杂,其实使用起来很简单,例如,一般用户可以充分利用 syn 标示来阻止未经授权的非法访问。比如当浏览网页时,系统会发送一个请求到 Web 服务器上,该服务器会响

应该请求并发回一个数据包，同时在系统中开启一个端口。和响应请求不同，Web 服务器并不关心其传输的内容，利用这个特点可以设置过滤规则，来阻止所有未经您的系统授权的 TCP 连接，例如执行“iptables t filter A INPUT i eth0-ptcp-syn jDROP”，其中的“-i”指的是网卡，“-p”指的是协议，“-syn”指的是带有 SYN 标识的 TCP 数据包。SYN 用于初始化一个 TCP 连接，如果自己的电脑没有运行任何服务器软件，别人就无法向您发送 SYN 数据包。

如果想拦截所有发送到本机的 ICMP 数据包的话，可以下执行命令“iptables A INPUTp icmp s0/0d0/0j DROP”。其中的“-p”参数指明控制何种网络协议，这里是 ICMP 协议。其中的参数“-s”表示源地址，后跟“0/0”表示任何源地址，其中的“-d”参数表示目标地址，后跟“0/0”表示所有的目标地址。其中的参数“-j”表示对符合条件的数据包采用何种处理办法，后跟

“REJECT”表示拒绝该数据包。如果本机是一台 Web 服务器，需要阻止外部主机对本机进行访问，可以执行命令“iptables A INPUT ptcp s0/0 d0/0 dport 80 j drop”，其中的“-dport 80”参数指明封锁本机的 80 端口。相反的，如果允许 IP 分为位“123.456.789.0/24”的外部主机访问本机所有端口，可以执行命令“iptables-A INPUT-s 123.456.789.0/24 d0/0j ACCEPT”，其中的“-jACCEPT”参数表示允许访问。当需要删除 iptables 创建的安全规则时，首先使用“iptables line-numbers nL”命令。来查询系统中的所有安全规则，每一条安全规则都存在一个编号，例如需要删除第 9 条规则，执行命令“iptables D INPUT 9”即可，其中的“-D”参数表示删除操作。当然，可以将一系列的 IPTables 规则放进一个初始化的 Shell 脚本里，并为其加上可执行属性，设置为开机运行状态，就可以组建一个功能强悍的防火墙。

多账户信息外泄防范

江苏 王根宏

预防跳转列表外泄

从 Windows 8 版本系统开始，新增的任务程序跳转列表功能，就给大家留下了耳目一新的感觉，但大家要是在单位或多用户账户环境下工作时，该功能可能会在不经意间，将大家的操作痕迹或重要信息外泄出去。所以，出于安全方面的原因，在公共场合下或多用户账户环境下，我们很有必要将这个新增的跳转列表记忆功能停用掉。

在进行这种操作时，首先用鼠标右键单击系统任务栏空白区域，点击右键菜单中的“属性”命令，进入系统任务栏属性对话框，选择“跳转列表”标签，在对应标签页面的“隐私”位置处（如图 1 所示），将“在跳转列表中存储并显示最近打开的项目”、“存储最近打开的程序”等选项前面的勾号取消掉，确认后保存设置操作。这样，就能达到预防跳转列表外泄功能目的了。

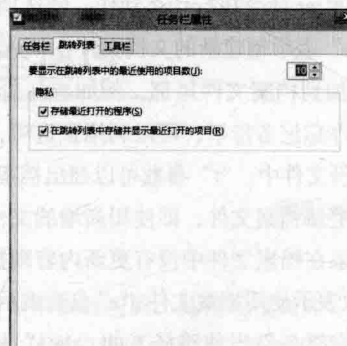


图 1 任务栏属性

预防特定程序外泄

在多用户账户环境下，很多应用程序都不允许使用，以免影响工作或引起信息外泄现象，工作人员可以通过系统注册表，来限制特定程序不能启动运行，从而达到预防特定程序外泄目的。

例如，为防止用户通过 QQ 程序将单位重要数据泄露出去，我们可以进行如下操作，来预防该应用程序对外泄露：依次单击“开始”、“运行”命令，弹出系统运行对话框，输入“regedit.exe”命令并回车，开启系统注册表编辑器运行状态。在该编辑窗口左侧列表中，依次展开注册表分支“HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Policies”(如图2所示)，用鼠标右键单击目标分支选项，逐一点击右键菜单中的“新建”、“项”命令，将新创建的项名称设置为“Explorer”。



图2 注册表编辑器

将鼠标定位到新创建的“Explorer”节点上，在该节点下面手工创建一个 32 位双字节键值，将该键值名称取为“DisallowRun”，同时将其数值输入为“1”，来禁止启动所有的应用程序，如果该键值数值设置为“1”时，则意味着本地系统将允许启动所有应用程序。

再次返回到“Explorer”节点上，打开该节点选项的右键菜单，依次选择“新建”、“项”选项，手工创建一个名称为“DisallowRun”的注册表子项，在该子项下面新建所要禁止启动的应用程序字符串键值，键值名称必须为连续的阿拉伯数字，例如“1”、“2”、“3”、“4”等，而数值必须为应用程序的 exe 文件名称，例如这里可以输入“qq.exe”。

重新启动计算机系统，让设置正式生效。这时，尝试在 Windows 系统中启动 QQ 程序时，系统将会弹出相关操作由于受到限制而被取消之类的提示信息，那么 QQ 程序将不能对外泄露本地系统的重要数据文件。

预防登录账号外泄

Windows 7 系统新增有登录监控功能，该功能可以让前一次登录系统使用的账号名称和登录时间，在下次登录操作时自动显示出来。很显然，在多用户账户环境下，这种功能特别容易泄露用户的登录隐私。为了预防自己的登录账号外泄，不妨对 Windows 7 系统进行如

下设置操作，来暂停对应计算机系统的登录监控功能：

首先使用“Win+R”快捷键，调用系统运行对话框，在其中执行“gpedit.msc”命令，开启系统组策略编辑器运行状态。在组策略编辑界面左侧显示窗格中，依次展开“本地计算机策略”、“计算机配置”、“管理模板”、“Windows 组件”、“Windows 登录选项”节点选项。

接着找到该节点下的“在用户登录期间显示有关以前登录的信息”组策略选项，用鼠标双击之，弹出如图3所示的组策略属性对话框，选中这里的“已禁用”选项，确认后保存设置操作。这样，就能成功关闭 Windows 7 系统的登录监控功，那么自己的登录账号信息就不容易对外泄露了。

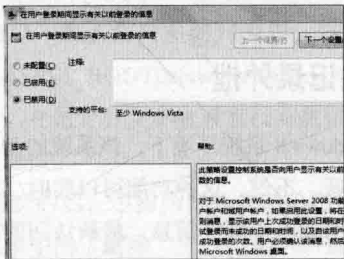


图3 组策略属性对话框

预防数据分区外泄

在多用户账号环境下，无论我们怎么小心谨慎，存储在特定磁盘分区中的数据文件，仍然有被其他用户偷窥的风险。为了预防重要数据文件外泄，我们可以使用系统管理员权限账号登录系统，打开系统注册表编辑器，来修改相关键值内容，达到隐藏当前用户磁盘分区目的。

例如，在隐藏系统分区时，可以依次单击“开始”、“运行”命令，弹出系统运行对话框，输入“regedit.exe”命令并回车，开启系统注册表编辑器运行状态。在该编辑窗口左侧列表中，将鼠标定位到注册表分支“HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Policies”上，打开该分支选项的右键菜单，依次选择“新建”、“项”命令，手工创建好“Explorer”子项。之后在“Explorer”子项下面，生成一个 32 位的“NoDrives”双字节键值，将该键值数值设置为十六进制的“4”(如图4所示)，确认后刷新系统注册表，让上述设置操作立即生效。这时，重新以刚才的用户账户登录时，用户就不能查看 C 盘分区中的所有数据文件了。

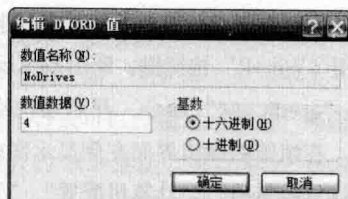


图4 编辑 DWORD 值

要提醒大家的是，随意修改系统注册表键值，容易损坏 Windows 系统的运行稳定性，所以，为了安全起见，在修改注册表键值之前，应当及时备份计算机系统中的所有重要数据，也可以通过系统还原功能，创建一个系统还原点，确保在问题发生的时候，能够通过系统还原点取消对计算机系统的调整。

预防磁贴记录外泄

在 Windows 8 系统环境下，该系统的动态磁贴功能让人耳目一新。不过，这种功能可以实时、动态地显示有关信息，例如电子邮件信息、最新访问的网站页面等等，这些信息在多用户账户环境下，会不经意地将用户的隐私内容外泄出去。实际上，用户每次执行计算机关闭操作的时候，想办法自动清理 Win8 系统的磁贴记录，就能有效预防磁贴记录外泄现象发生，下面就是详细的操作步骤：

首先使用“Win+R”功能键，打开系统运行对话框，在其中执行“gpedit.msc”命令，开启系统组策略编辑器运行状态。在该编辑界面的左侧显示窗格中，将鼠标定位到“本地计算机策略”、“用户配置”、“管理模板”、“开始菜单和任务栏”分支上，选中该分支下的“退出系统时清除瓦片通知的历史记录”选项，同时用鼠标双击该组策略选项，弹出如图 5 所示的组策略属性对话框。

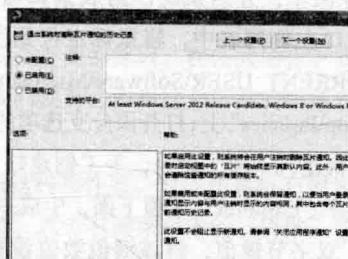


图5 历史记录

其次看看“已启用”选项有没有被勾选，如果发现其还没有被勾选时，必须立即将其重新选中，单击“确定”按钮保存设置操作。这样，日后用户每次执行计算机系

统关闭操作时，动态磁贴中的历史记录内容，就会被自动清理干净了，那么磁贴记录功能当然不会对外泄露隐私了。

预防搜索功能外泄

与 Windows XP 之类的操作系统相比，Windows 7 系统的文件搜索功能智能化程度很高，但是该功能在搜索操作结束后，会将搜索关键字记忆保存在搜索文本框中，这在多用户账户环境下，很容易带来隐私外泄的风险。为了预防搜索功能对外泄密，我们不妨进行如下设置操作，来暂时关闭搜索记录保留功能：

在关闭搜索记录保留功能之前，必须先将已经存在的搜索痕迹抹除掉。考虑到 Windows 系统没有提供直接删除搜索痕迹的功能，即使使用一些外力工具也不能删除，这时只有通过注册表才能完成删除任务。依次单击“开始”、“运行”命令，在系统运行对话框中执行“regedit”命令，开启系统注册表编辑器运行状态。在该编辑窗口左侧列表中，将鼠标定位到如图 6 所示的注册表分支“HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Explorer\WordWheelQuery”上，所有搜索痕迹记录都会出现在该分支下面，只要将除了名为默认的项全部删除，再重新启动计算机系统即可。



图6 注册表分支

接着就能暂时关闭搜索痕迹自动记忆功能了。依次单击“开始”、“运行”命令，在系统运行对话框中执行“gpedit.msc”命令，弹出系统组策略编辑界面。在该编辑界面左侧显示窗格，将鼠标定位到“本地计算机策略”、“用户配置”、“管理模板”、“Windows 组件”、“Windows 资源管理器”节点上，找到该节点下的“在 Windows 资源管理器搜索框中关闭最近搜索条目的显示”选项，并用鼠标双击之，切换到对应选项设置对话框，选中“已启用”选项，确认后保存设置操作。这样，就能达到暂时关闭搜索保留功能，预防该功能对外泄密目的了。

预防文件历史外泄

大家知道, Windows 8 系统新开发出文件历史记录功能, 它能自动对存储在系统桌面、联系人文件夹、系统收藏夹、库等位置处的隐私信息进行备份。其实, 在多用户账户环境下, 文件历史功能实用价值并不是很大, 因为它无法对其他路径处的数据文件进行自动备份, 而且它的存在还会带来隐私外泄的风险。为了预防 Windows 8 系统文件历史记录功能外泄风险, 我们可以进行如下设置操作, 临时关闭运行该功能:

首先依次单击“开始”、“运行”命令, 在系统运行对话框中执行“gpedit.msc”命令, 开启系统组策略编辑器运行状态。在该编辑界面左侧显示窗格中, 将鼠标定位到“本地计算机策略”、“计算机配置”、“管理模板”、“Windows 组件”、“文件历史记录”分支上。

选中该分支下的“关闭文件历史记录”选项, 打开该选项的右键菜单, 点击“编辑”命令, 弹出如图 7 所示的组策略属性对话框, 将“已启用”选项勾选起来, 单击“确定”按钮保存设置操作。这样, Win8 系统的文件历史记录功能, 日后将不会对系统收藏夹、库、系统桌面、联系人文件夹等路径处的隐私数据自动备份, 那该功能自然也就不会对外泄露了。

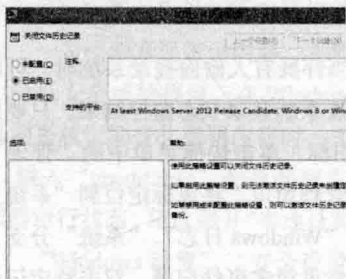


图 7 组策略属性对话框

预防共享访问外泄

在局域网工作环境中, 终端计算机系统相互进行共享访问, 是十分常见的事情。但细心的用户会发现, Windows 7 系统在设置共享文件夹时, 会以“两个小人”图标区分共享文件夹和普通文件夹, 这容易让别人通过这样特殊的共享标志, 轻松偷窥到重要的共享隐私, 从而发生共享访问外泄现象。

为了避免这种现象发生, 我们不妨进行如下操作, 取消共享文件夹的“两个小人”图标, 让其他用户无法分辨出哪些文件夹是共享文件夹:

首先逐一点选“开始”、“运行”选项, 弹出系统运行对话框, 在其中执行“regedit”命令, 展开系统注册表编辑窗口。在该窗口左侧列表中, 将鼠标定位到“HKEY_CLASSES_ROOT\Network\SharingHandler”注册表分支上, 在指定分支下查看有没有数值为“ntshrui.dll”的默认键值。

如果找到的话, 不妨用鼠标右键单击该默认键值, 点击右键菜单中的“删除”命令, 确认后重新启动计算机系统, 这样共享文件夹图标上面的“两个小人”标志就会自动消失了。当我们自己也不能识别出哪些是共享文件夹时, 可以进入 DOS 提示符窗口, 输入“net share”命令, 就能找到本地系统中的所有共享文件夹了。

事前设防“做主”登录安全

江苏 王凯

强化登录安全提醒

在公共计算机操作环境下, 为了防止一些共用者不

遵守操作规定, 随意修改系统设置, 降低系统安全防护能力, 我们可以进行适当设置, 让其成功登录系统后, 及时看到一些安全提示。在 Windows 系统环境下, 要做

到这一点,可以进行下面的设置操作,让用户登录成功后,可以直接看到“不得擅自修改系统设置”之类的安全提醒:

首先依次单击“开始”、“运行”命令,弹出系统运行对话框,输入“regedit”命令并回车,开启系统注册表编辑器运行状态。在该编辑窗口左侧,逐一跳转到 HKEY_LOCAL_MACHINE/SOFTWARE/Microsoft/Windows NT/CurrentVersion/Winlogon 注册表分支上,如图 1 所示。



图 1 注册表编辑器

接着用鼠标双击指定分支下的“LegalNoticeCaption”注册表键值,展开“数值数据”编辑对话框,输入“登录安全提醒”,再双击指定分支下的“LegalNoticeText”键值,同时将该键值数值内容修改为“登录系统后请不要自由调整设置”,按“确定”按钮退出编辑对话框,再重新启动计算机系统即可。

严密监控登录状态

在公众场合下,严密监控系统登录状态,包括追踪监控每位用户登录系统的状态信息,可以及时、准确地揪出幕后登录黑手。对于 Vista 以后版本系统来说,进行这种监控操作很简单,只要启用 Windows 系统的登录监控功能,就可以在下次成功登录系统时,监控到上一次登录状态信息,根据这样的监控结果,就能识别出是否有人偷偷登录过本地系统。在启用该功能时,逐一点击“开始”、“运行”命令,弹出系统运行文本框,输入“gpedit.msc”命令并回车,展开系统组策略编辑界面。将鼠标定位到“本地计算机策略”、“计算机配置”、“管理模板”、“Windows 组件”、“Windows 登录选项”节点上,找到指定节点下的“在用户登录期间显示有关以前登录的信息”选项,进入对应选项设置对话框,勾选“已启动”选项,确认后保存设置操作即可。日后,如果有人悄悄登录计算机时,Windows 系统就会将它们的登录系统状态监控到,并且存储下来,根据该结果就能知道

是哪个用户账号执行登录操作的。

如果希望监控到更多的状态信息时,可以通过 Windows 系统内置审核登录功能,来自动追踪每次登录系统的详细信息,即使登录系统操作失败了,Windows 系统也能监控到这个过程。在进行该监控登录操作时,先要审核系统登录成功、失败操作事件。只要依次单击“开始”、“运行”命令,在弹出的系统运行文本框中,执行“secpol.msc”命令,打开系统本地安全策略控制台窗口。逐一跳转到该窗口的“安全设置”、“本地策略”、“审核策略”分支上,双击指定分支下的“审核登录事件”选项,切换到如图 2 所示的选项设置框,勾选“成功”、“失败”等选项,确认后退出设置对话框即可。

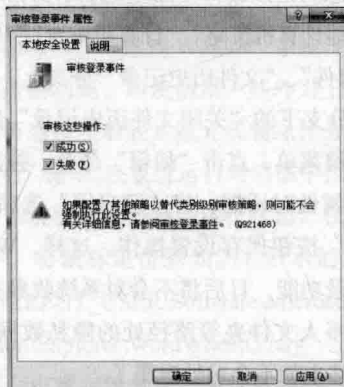


图 2 选项设置框

日后,当怀疑有人偷偷登录系统时,可以打开事件查看器,查看系统登录状态监控结果。只要用鼠标右击“计算机”图标,单击快捷菜单中的“管理”命令,切换到计算机管理窗口。将鼠标定位到“系统工具”、“事件查看器”、“Windows 日志”、“系统”分支上,在指定分支下将能看见很多事件记录,双击特定记录选项,在其后界面中就能查看到包括登录账号名称、登录系统时间等更多的状态信息。

强行使用登录密码

为了增强系统登录安全性,微软早期通过 Ctrl+Alt+Del 组合键,强制用户打开系统登录对话框,只有正确输入登录密码才能顺利进入系统界面。但后来,微软从操作方便性出发,停用了默认状态下强制输入登录密码的功能。这在登录安全要求较高的情况下,显然是不能容忍的,为了防止恶意登录现象出现,可以进行如下操作,来重启强制输入登录密码功能:依次单击“开始”、“所有程序”、“附件”、“运行”命令,展开系统运

行文本框，输入“netplwiz”命令并回车，从其后弹出的界面中点选“用户”选项卡，在对应选项设置页面中，勾选“要使用本机，用户必须输入用户名和密码”，按下“添加”按钮，导入合法可信用户账号，单击“确定”按钮保存设置操作。

之后单击“高级”选项卡，打开如图 3 所示的选项设置页面，在“安全登录”设置项处，勾选“要求用户按 Ctrl+Alt+Del”选项，单击“确定”按钮退出设置对话框。重启计算机系统后，在登录系统前，用户将看到要按 Ctrl+Alt+Del 键才能登录系统的提示。经过实践检验，借助 Ctrl+Alt+Del 组合键，强行输入登录密码，可以从根本上解决非法用户通过字典来暴力登录系统的现象。

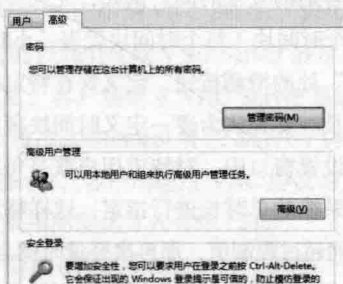


图 3 选项设置页面

为了保证登录密码拥有更好的安全防护效果，还要做好下面两点：一是强制变换密码内容。不停地变化密码内容，可以降低安全威胁程度。在 Windows XP 系统环境下，要强制系统定期变化密码内容时，先展开系统运行对话框，输入“gpedit.msc”命令并回车，开启系统组策略编辑器运行状态。依次展开“本地计算机策略”、“计算机配置”、“Windows 设置”、“安全设置”、“账户策略”、“密码策略”分支，双击该分支下的“密码最长存留期”选项，弹出如图 4 所示的选项设置对话框，输入合适的密码变换间隔时间，例如输入“20”，确认后保存设置操作，Windows 7 系统日后会每隔 20 天就提示用户更改密码内容。

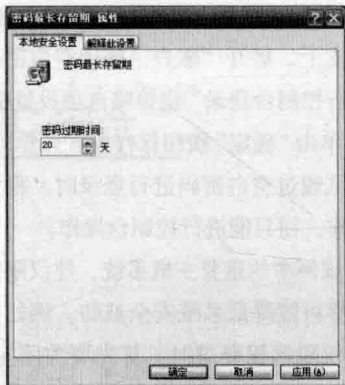


图 4 选项设置对话框

二是限制密码最小位数。前面本文提到，一个高强度、复杂化的密码所包含字符应该不少于 12 个，管理员级别的密码字符数尽量要达到 15 个字符。要进行这种限制操作时，可以打开系统组策略编辑器窗口，在该窗口的左侧列表中，将鼠标定位到“本地计算机策略”、“计算机配置”、“Windows 设置”、“安全设置”、“账户策略”、“密码策略”分支上，双击该分支下的“密码长度最小值”选项，弹出密码长度最小值设置框，在其中输入“12”，确认后密码最小位数将不能低于 12 个字符。

严格限制登录方式

不同性质的系统平台，可能对登录方式有不同的限制要求，如果同时允许多种登录方式，显然就会多一份安全威胁。例如，在单位内网环境中，有些不怀好意的用户或许会使用网络登录方式，悄悄破坏内网中的共享数据。为了避免这种不安全现象，我们可以在共享数据所在主机系统中，限制用户使用网络登录方式。只要打开系统运行文本框，执行“gpedit.msc”命令，将鼠标定位到系统组策略编辑器中的“本地计算机策略”、“计算机配置”、“Windows 设置”、“安全设置”、“本地策略”、“用户权限分配”分支上，展开“拒绝从网络访问这台计算机”组策略选项设置框。删除所有已经存在的用户账号，之后按下“添加用户或组”按钮，导入不允许使用网络登录方式的用户账号，单击“确定”按钮保存设置操作即可。

在公共场合下，建议限制空白密码账号的登录方式，让其只允许使用控制台登录方式，否则容易给网络中的重要系统带来致命威胁。在进行这种限制操作时，只要在系统运行对话框中执行“gpedit.msc”命令，将鼠标定位到系统组策略编辑器的“本地计算机策略”、“计算

机配置”、“Windows 设置”、“安全设置”、“本地策略”、“安全选项”分支上,展开“账户:使用空白密码的本地账户只允许进行控制台登录”组策略选项设置框,勾选“已启用”选项,单击“确定”按钮保存设置操作即可。日后,任何用户尝试通过空白密码进行登录时,将无法进行正常的访问操作,而只能进行控制台操作。

对于局域网中的重要主机系统,建议限制其远程登录方式,以尽可能降低系统安全威胁。例如,要限制他人以管理员权限远程登录时,首先要关闭 administrator 账号缺省远程登录权限。只要先进入系统运行文本框,执行“cmd”命令,在 DOS 窗口命令提示符下,输入“net user administrator /active:no”命令即可。接着仅为合法账号赋予远程登录权限,只要右击系统桌面上的“计算机”图标,点选右键菜单中的“属性”命令,弹出系统属性对话框,单击“远程设置”按钮,在远程设置页面的“远程桌面”处点击“选择用户”按钮,展开远程桌面用户设置框(如图 5 所示)。删除所有已经存在的用户账号,单击“添加”按钮,导入合法用户账号,确认后保存即可。

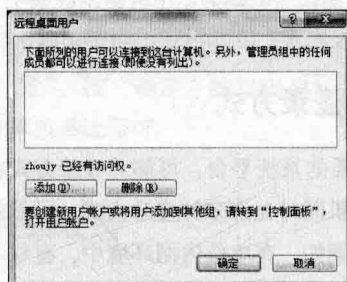


图 5 远程桌面用户设置框

加强登录时间管控

我们知道,在正确输入用户账号和密码的情况下,系统登录操作一般会很顺利。可是,在特定工作环境下,例如在服务器环境下,如果允许每位用户无限制登录服务器系统,不但容易造成系统性能下降,而且可能带来更多的潜在风险。所以,有时我们需要为不同的用户账号设置合适的登录使用时间。

这里,大家可以使用“User Time Control”这款外力工具,对服务器系统中的用户账号进行登录时间限制,同时可以进行登录权限限制。先从网上下载安装“User Time Control”工具,开启它的运行状态,展开如图 6 所示的主程序窗口,逐一点选“Edit”、“Programs

Options”命令,进入程序设置框,单击“Administrator Password”按钮,定义好程序管理密码,让系统管理员才有资格管理用户的系统登录时间。

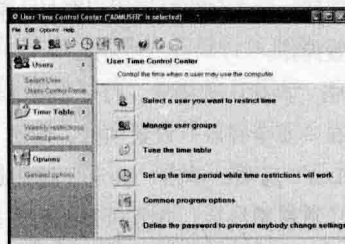


图 6 主程序窗口

之后逐一点选“Edit”、“User Control Pannel”命令,在用户账号设置框中选中标用户账号,在其后界面中按需设置好合适的登录时间。例如,先在时间表格中勾选一个或多个时间块(每个时间块代表一小时),接着移动“Minutes”处的滑动按钮,定义好在特定时间块内限制登录的时长。要是认为逐一时间块很麻烦时,不妨在下一步设置窗口中,对特定用户账号每次、每天或每星期登录系统的总时长进行指定,这样特定用户如果登录系统时间超过限制值,那再次登录时就会发生错误。

接下来要对特定用户登录系统后所能进行的操作权限进行定义,保证无关用户不能在重要系统中自由操作,以避免系统被非法破坏。可以定义的操作权限一般包括:拒绝安装非法软件、拒绝调整系统时间、拒绝使用进程管理器、拒绝添加/删除应用程序、拒绝修改用户账号信息等。一般情况下,应该拒绝用户调整系统时间,以防止事先设定的系统登录时间无效。

限制登录权限

相信重要计算机系统中都可能保存一些非常隐私的数据,而这些数据信息,要是不小心被其人偷窥到,或许会带来严重的安全威胁。其实,平时对重要隐私数据进行加密,就能有效避免普通登录用户随意访问它们。加密操作相当简单,只要先进入系统资源管理器窗口,找到需要加密的数据文件所在文件夹,打开它的快捷菜单,选择“属性”命令,弹出目标文件夹属性设置框,点击“高级”选项卡,进入高级选项设置框,勾选“加密内容以便保护数据”,确认后保存设置操作,这样就能完成加密操作。经过这种加密保护后,其他人在偷偷访问被保护的隐私数据时,就需要通过身份验证,验证不通过就无权访问了。



SSH 转发保 VNC 安全

河南 刘景云

VNC 的基本功能与操作

为了便于远程管理 Linux 服务器,可以使用 VNC 技术来实现,VNC 软件由 VNC Server 和 VNC Client 两部分组成,分别用于服务器和客户端,其过程是客户端通过 VNC Viewer 连接到 VNC Server,VNCServer 要求输入连接密码以及存/取 VNC Server 显示装置,当密码验证通过后,客户端要求 VNC Server 显示桌面环境。VNC Server 通过 X Protocol 要求 XServer 将显示控制权交给 VNC Server,客户端通过 VNC 协议与 VNC Server 进行通讯,采用图形化方式管理 Linux。

在服务器端执行“vncpasswd”命令,设置连接密码,密码保存在用户主目录中的特定文件中,例如“/root/.vnc/password”。执行“vncserver: 1”命令,可以启动 VNC 服务,其中的“1”表示桌面编号,当然也可以设置为别的桌面编号。注意,与桌面 1 对应的端口为 5901,与桌面 2 对应的端口是 5902,之后以此类推。如果启用了防火墙的话,需要开放这些端口。如果初次使用该命令,之前没有设置密码的话,系统会要求输入密码,之后客户端就可以利用 VNC Viewer 等工具,执行连接操作。

例如执行“vnc viewwe 192.168.1.10: 1”命令,输入 VNC Server 的地址和密码,就可以连接服务器了。为了以图形方式连接,可以打开“/root/.vnc/xstartup”文件,将最后一行的“twm”修改为“gnome-session”或者“startkde”,前提是系统已经安装了 Gnome 或者 KDE 桌面。也可以将最后两个注释符号删除,使该 VNC 虚拟桌面按普通桌面启动。修改完毕后,执行“vncserver kill: 1”、“vncserver: 1”,来重启 VNC Server,之后重新连接 VNC 服务器,就可以显示 Gnome 或者 KDE 桌面环境。

SSH 的基本功能与操作

在 Linux 中使用最广泛的是 OpenSSH 加密工具,执行“rpm aq|grep ssh”命令,可以查看 OpenSSH 软件包的安装情况。如果没有安装的话,在服务器上执行“rpm-ivh openssh-4.3p2-26.el5.i386.rpm”之类的命令进行安装操作,执行“tar xzvf openssh-x.xpl.tar.gz”、“cd openssh-x.xpl”、“make”、“make install”等命令,安装最新的 OpenSSH,“openssh-x.xpl.tar.gz”为具体的版本号。

执行“chkconfig level 2345 sshd on”命令,可以让 sshd 服务器开机自动运行。执行“service sshd start”或者“service sshd stop”命令,可以启动或者关闭 OpenSSH。在“/etc/ssh/sshd_config”文件中保存 OpenSSH 服务器端配置信息,在“/etc/ssh/ssh_config”文件中包含其客户端配置信息,用户可以根据实际情况对其进行修改。为了避免风险,最好禁止 Root 账户登录 OpenSSH,在“/etc/ssh/sshd_config”文件中将“PermitRootLogin”的值设置为“no”即可。当初次登录 SSH 服务器时,执行“ssh l user01 192.168.1.10”,假设 SSH 服务器的 IP 为 192.168.1.10,根据提示输入“yes”,接受服务器发来的 RSA 密钥,并将其保存在本例的“~/.ssh/known_hosts”主机列表文件中,之后输入账户密码,就可以连接到 SSH 服务器上。

添加了 SSH 主机密钥后,以后登录就不会出现警告信息,使用者可以在 SSH 主机的 Shell 提示符下执行各种命令了。利用 scp 命令,可以执行文件安全复制操作,例如执行“scp data.c @192.168.1.10:/code”命令,当接受 SSH 服务器密钥,输入账户密码后,可以将本地的“data.c”文件复制到 SSH 服务器中的“/code”目录。执行“scp-r/home/shuju user01@192.168.1.10:/share”命令,可以将“/home/shuju”目录完整复制到服务器中。scp 命令是先调用 SSH 进行登录,之后复制文件,最后调用 SSH 关闭这个连接。

为了便于在 Windows 下连接 SSH 服务器,可以使

用 SSH Secure Client 这个小工具来实现。在其主界面工具栏上点击“Quick Connect”按钮,输入 SSH 服务器地址、账户名、端口等内容,点击“Connect”按钮,当接受密钥信息,输入账户密码后,就可以在其中自由执行各种命令,对服务器进行远程管理。点击工具栏上的“New File Transfer Window”按钮,在文件传输界面中可以使用拖拽等方式,灵活地在本地和 SSH 服务器之间传输文件。

使用 SSH 转发,为 VNC 开启加密通道

VNC 的特点之一是可以对数据进行压缩,因此其传输的数据量相对于 SSH 加密传输来说要小得多。但是 VNC 并非完美无缺。

要想使用 SSH 保护 VNC 安全,即利用 SSH 为 VNC 开辟加密通道,需要使用 SSH 的端口转发功能,即用户可以在本地端口和远程服务器端口上运行的某服务的端口之间建立安全通道,所有对本地端口的请求都

被 SSH 加密,并转发到远程服务器的端口。

在本地执行“vncviewer 192.168.0.100:1”命令,就可以将 VNC 连接完全至于 SSH 的加密通道中,无论是传输的账户名密码,还是具体的数据,黑客是无法进行监听的。为了便于在 Windows 中使用 VNC 连接,也可以借助于上面谈到的 SSH Secure Shell 来实现 SSH 端口转发功能。在该软件主界面工具栏上点击“Settings”按钮,在设置界面左侧点击“Tunneling”项,在右侧点击“Add”按钮,在弹出窗口中的“Display”栏中输入连接项目名称,在“Listen”栏中输入本地监听端口,例如 5902。在“Destination”栏中输入服务器 IP,在窗口底部输入服务器 VNC Server 端口。点击 OK 按钮保存转发配置信息,之后利用 VNC Viewer,就可以进行安全连接了。例如 Windows 下的 View Viewer 程序,在其连接界面的目标的“Server”栏中输入“localhost:5902”,点击确定按钮,输入账户名和密码,就可以安全连接 VNC 服务器了。

加强无线网络安全性

河南 郭振江

无线网络安全机制

现在的无线网络都是基于 WPA/WPA2 安全性标准,WPA (即 WiFi Protected Access, WiFi 网络安全存取)可以有效保护无线网络的数据安全,提高介入控制的安全性级别,通过采用 TKIP (临时密钥完整性协议),建立一种动态密钥机密和相互验证的安全机制,使用密钥与网络上的不同设备的 MAC 地址及更大的初始化向量合并,让每个网络节点都使用一个不同的密钥流对其数据进行加密,之后 TKIP 会使用高强度加密算法对数据进行加密,而且 TKIP 修改了常用的密钥,有力地保证了网络的安全性。

WPA 的特点之一是使用动态密钥,密钥时刻处于变换中,因此 WPA 是目前无线网络安全性最高级别之一。WPA 包含 WPA-PSK 和 WPA-Enterprise 两个版本,

前者主要针对小型网络设计,其使用名为 PSK (即 Pre-Shared Key,预共享密钥)的密码,该密码越复杂,无线网络的安全性就越高。后者用于提高企业网的安全性,WPA 提供了完整性检查功能,来确保密钥未受到恶意攻击,加强了用户认证功能,包含了对 802.1X 和 EAP 可扩展协议的支持,其中的 EAP 用于验证过程中的消息交换,它通过外部的 RADIUS 远程验证拨入用户服务,对无线用户进行安全认证,也可以在以太网中使用 RADIUS 协议自动更改和分配密钥。

WPA2 是第二代 WPA,其向后兼容于支持 WPA 的产品,两者主要区别在于 WPA2 使用更加高级的加密算法对数据加密,WPA2 也分为 WPA2-Enterprise 和 WPA2-Personal 版本。在常见的无线路由器设置界面中,在无线安全模块里,可以采用 WPA-PSK 或者 WPA2-

PSK 安全模式，并分别提供了 AES 和 TKIP 等加密规则可供选择。同 TKIP 相对较弱的加密功能相比，AES 是一个迭代的、对称密钥分组的密码，它可以使用 128、192 和 256 位密钥，并且用 128 位（16 字节）分组加密和解密数据。

AES 提供了比 TKIP 更加高级的加密技术，而且在使用 TKIP 算法时路由器的吞吐量会下降得比较严重，所以一般都是选择 AES 加密规则。WPA 虽然安全性很高，加强了生成加密密钥的算法，即使攻击者收集到了分组信息并进行分析，也很难算出通用密钥，但是其并非无懈可击，因为它采用了较为薄弱的加密算法，攻击者只要监听到数量够多的数据包，凭借着功能强悍的破解工具，也可以突破 TKIP 的保护，破解并侵入无线网络。

无线安全面临的威胁

例如黑客使用 Aircrack-ng、Cowpatty 等工具，通过进行 Deauthenticate 验证攻击，迫使 AP 和客户端重新进行握手验证来截获握手验证数据包，当得到握手数据包后，攻击者会使用密码字典，执行 WPA-PSK 的密码破解操作，根据密码的复杂度，破解时间可以是几分钟、几小时或者数天不等，只要攻击者有耐心，破解无线网络并非难事。值得说明的是，Deauthenticate 功能往往需要多次进行才能成功，对数据包进行反复拦截，会造成在攻击进行过程中，目标 AP 和无线客户端之间无法正常通讯，出现频繁断网的情况。即使对于安全性更高的 WPA2 标准，仍然存在被破解的风险，例如在 Ubuntu 下，使用特定的无线网卡（例如 Linksys USB 网卡），配合最新版本的 Airdump-ng 程序，利用 Deauth 验证攻击，同样可以截获 WPA2 握手数据包，黑客利用密码字典，对数据包进行破译，完全可以破解其密码。值得注意的是，在执行针对 WPA2 的 Deauth 攻击时，为了保证成功率需要进行反复拦截，很可能导致目标 AP 和别的客户端频繁断网，对于低端的 AP 必须重启才行。使用 Wireshark 等工具，对截获的 WPA2-PSK-AES 数据包进行分析，可以清楚其采用的是 AES 加密规格，密钥的长度为 16，对 WPA2-PSK-PKI 数据包进行分析，可以看到其采用的是 RC4 加密规格，密钥长度为 32。

设置复杂密码 抗击非法破解

大量的黑客入侵案例证明，WPA/WPA2 安全标准并

非坚不可摧，我们必须采取各种措施来强化无线网络的安全性。最重要的是在 WPA/WPA2 上设置复杂的密码，不给黑客可乘之机。当黑客破解无线网络时，会有针对性地制作一些密码字典，黑客需要利用这些密码字典来破解无线网络密码。因此，在设置密码时，要遵循一些方法和技巧。例如密码的长度要超过 8 位，尽量不要使用固定的单词、人名、词组、生日等规律性较强的密码，密码中应该同时包含 3 种以上的大小写字母、特殊符号等元素，要养成定期更换密码的习惯，增大黑客破击的难度。

其实，在实际设置密码时，我们经常采用字符串加数字的方式，例如对于“beijing19810109”来说，黑客破解起来并不复杂，如果将其中的字母和数字混编起来，例如将其修改为“1b9e8ilj0i1n0g9”，其密码强度就大大提高了。要想依靠字典破解这样的密码，恐怕需要花费很长的时间。很多用户习惯于设置某个单词作为密码，其安全性就比较低。例如对于“helloworld”来说，破译起来就很简单。如果将其中的某些字母进行替换处理，例如将“h”替换为“in”，第一个“o”替换为“（）”，“w”替换为“1vi”，第二个“o”替换为“@”，“r”替换为“7”，“d”替换为“/v”。那么修改后的密码就会变成“inell（）1vi@7l/v”，无疑会大大提高密码的复杂度。如果对较长的密码进行此类替换修改，黑客就得花费几年甚至更长时间进行猜测破译。

在设置密码之前，最好对其强度进行测试，例如打开网址“<http://www.microsoft.com/zh-cn/security/pc-security/password-checker.aspx>”，在密码检测器页面（如图 1 所示）中的“password”栏中输入密码，在“Strength”栏中显示以色彩和说明文字表示该密码的强度，例如绿色表示很弱，黄色表示一般，绿色表示强壮。例如对上述“inell（）1vi@7l/v”密码进行测试，显示绿色的“Strong”字样，表示其是合格的密码。当然，对于 14 位以上并且使用三种或者四种字母、数字、特殊字符组合的密码，会显示“Best”字样，表示其为最佳的密码。对于普通的个人用户来说，在设置 WPA/WPA2 密码时，其强度应该达到“Strong”级别，对于安全性要求很高的企业网来说，其密码强度应该达到“Best”级别。



图1 测试密码安全性

在黑客对无线网络进行破解时，往往出现快速破解 WPA 密码的情况。按照常见的方法，黑客会先有针对性地建立密码字典，之后对拦截的数据包进行破解，而很多用户的安全观念并不强，往往使用生日或者简单的单词作为密码，这样就很容易被破解。不过，按照字典破解的效率来说，其破解速度是很有限的，例如当用户采用由小写字母和数字组成的密码，假设黑客破解的效率是每秒测试 1000 个密码的话，那么理论上其需要 26 天的时间，才可以破解密码。如果用户的密码长度为 10 位的话，理论上黑客需要 117000 年才可以破解。

因此，如果用户采用复杂密码的话，按照常规的破解方法，黑客是无法破译密码的。打开“<http://lastbit.com/pswcalc.asp>”，在其中的“Password length”栏中输入密码长度，在“Speed”栏中输入破译的速度，单位为密码数/秒。在“Number of computers”栏长输入主机数量，一般为单机，在其下选择密码的组成，包括小写字母、大写字母、数字、标点符号、全 ASCII 等，点击“calculate!”按钮，可以测出破解所需要的时间。

抗击快速破解的技巧

当然，抗击非法破解的最有效的方法是强化 WPA/WPA2 密码强度，在黑客制作 WPA 密码表时，其设计的密码只包括数字、字符、标点符号等。我们反其道而行之，在密码中加入不可直接输入的非常规字符，例如利用输入法提供的软键盘，在密码中输入“★○◆□”等特殊的符号，那么 WPA/WPA2 的密码强度无疑会大大提高，即使黑客使用 WPA 密码表对其进行破解也毫无办法。

因为在建立 WPA 密码表是必须获得目标 AP 的 SSID 标识符，所以为了安全起见，可以每隔一段时间，对 SSID 进行一次修改，同时更改 WPA/WPA2 密码。很多无线产品会默认使用品牌的名字作为 SSID，例如

Mercury, TP-Link 等，应该及时对其进行修改。为了安全起见，不要使用归于简单的单词作为 SSID 名称，应该使用不太常用的单词或者组合词作为其名称。对于安全性要求较高的企业网来说，可以采取在无线网络中部署 RADIUS、VPN 等安全认证体系，对登录的用户尽行必要的安全认证，来提高无线网络的安全性。

搭建 VPN 环境

接下来介绍如何组建和使用无线 VPN，VPN 全称是 Virtual Private Network，即虚拟专用网，VPN 可以建立私有的安全通信信道，使远程用户可以稳定安全地连接到企业内网中，VPN 网络由虚拟专用网服务器、VPN 客户端、LAN 远程访问及隧道协议等组件构成。对于普通的 AP 来说，因为其采用无线传播的方式，在众多的监听和破解工具面前，其安全性无法得到保证。为此，可以将 AP 放置到内网的某一网段中，并使用防火墙将该网段保护起来，其作用是避免内网的其他网段用户与该 AP 建立非法连接，让目标可以使用虚拟专用网软件，来和该 AP 建立连接，这样无线网络的安全性可以得到明显提高。

如果在内网中存在 DMZ 非军事化区，作为非安全系统和安全系统之间的缓冲区的话，也可以将 AP 放置到该区域中。基于无线的 VPN 和传统的有线网络 VPN 很相似，所不同的是其通过 AP 或者无线路由器的中转，让外部客户可以通过 VPN 连接到内网，来访问内网资源，将虚拟专用网和无线 AP 结合起来，可以用多种模式来实现。例如，可以将 AP 连接到某台服务器的接口上，使用 Windows 内置的虚拟专用网络软件扩展无线通讯的范围，其优点是无需增加额外的硬件成本，实现起来很容易，缺点是增加了现有服务器的负担。

也可以采用内置了虚拟专用网网关服务的无线 AP，即将普通 AP 和虚拟专用网功能集成在一起，这样布设安装配置管理都比较简单，让每个无线连接都通过虚拟专用网实现连接，加密安全性得到了有力保证。缺点是需要购买价格昂贵的设备，无法满足新的无线局域网的需求等。也可以在 DMZ 非军事区指定一个服务器，专门处理和无线连接、VPN 网关、防火墙信息、开启关闭无线网络相关的管理事务。在 DMZ 中增加一个虚拟专用网，可以提高机密信息传输的安全性。

这里为简单起见，介绍在 Windows Server 2003 中组建无线 VPN 服务器的方法。打开路由和远程访问服务

器程序, 点击下一步按钮, 在向导窗口中选择“远程访问(拨号或VPN)”项, 在下一步窗口中选择“VPN”项, 点击下一步按钮, 在VPN连接窗口中选择外部工作网卡, 在下一步窗口中选择“来自一个指定的地址范围”项, 来设定VPN客户在执行远程访问后获得的IP地址。如果有DHCP服务器的话, 可以选择“自动”项, 在下一步窗口中设置所需的IP范围, 例如192.168.10.10到192.168.10.50等, 在下一步窗口中选择“否, 使用路由和远程访问来对连接请求进行身份验证”项, 点击完成按钮, 完成对PPTP VPN服务器设置操作, 之后系统会自动启动路由和远程访问服务。

为了便于客户端连接到内网中的VPN服务器, 需要对无线路由器进行必要的设置。在路由器设置界面中选择对应的上网方式, 包括拨号上网、小区宽带和专线上网等。在LAN口设置模块中, 设置路由器在内网中的IP地址, 例如192.168.0.1等。为了便于客户端使用, 需要将内网中的VPN服务器映射到外网, 在虚拟服务器模块中将内网VPN的1723端口映射到外网, 因为PPTP服务使用的是该端口。为了防止黑客的攻击, 有些路由器还可以设置允许访问该映射的时间段, 可以将其设置为白天时间段, 避开黑客活动频繁的夜晚时间段。这样, 内网的VPN服务器就被映射到了外网, 客户端只要连接该无线路由器, 就可以通过其访问内部的VPN服务器。当然, 事先应该建立连接的账户名, 为其设置密码, 并在其属性窗口中的“拨入”面板中的选择“允许访问”项。

在客户端的电脑上新建一个网络连接, 选择“连接到工作区”项, 在下一步窗口中选择“通过Internet使用虚拟专用网络(VPN)来连接”项, 在下一步窗口中输入目标主机名称或者IP地址以及连接的名, 并设置连接用户名和密码, 完成连接项目的创建操作, 双击该连接项目, 就可以连接到目标VPN服务器。当连接成

功后, 在CMD窗口中执行“ipconfig”命令, 可以显示本机无线网卡当前的和与远程VPN服务器建立连接后获得的IP地址。在VPN服务器上打开路由和远程访问控制台界面, 在端口列表中双击状态为“活动”的端口。可以查看登录用户名、验证状态、登录时间、数据包传输状态、使用的IP等信息。当然, 这是最常见的PPTP VPN的实现方法, 其他的更加高级的IPSEC、L2TP、SSL VPN的实现方法与之类似。

保护无线VPN的技巧

我们一般认为, VPN环境已经具有相当高的安全性, 可以保证数据安全稳定的传输, 不过事实却没有这么简单, 不管对于最常用的PPTP和强化的IPSec VPN, 还是大型网络使用的SSL VPN来说, 不管是有线还是无线环境, 都面临着各种恶意攻击的威胁。例如, 对于无线PPTN VPN环境来说, 黑客会使用Zenmap等工具来扫描VPN设备, 并利用ettercap等工具拦截VPN交互数据包, 在其中包含了用户名和加密的Hash信息。黑客使用asleap等工具, 配合密码字典, 可以破译拦截的数据包, 获得VPN连接密码。

对于安全性更高的IPSec VPN来说, 黑客会使用诸如IPsecScan等专用工具, 来扫描特定的地址段, 探测使用IPsec的设备。利用IKE-Scan, 可以对目标IP进行深度探测分析, 获得其加密方式、PSK预功效验证、操作系统类型等相关数据。利用Cain等工具, 对拦截的PSK预共享验证散列进行破解, 得到账户名密码等信息。因为破解操作需要使用密码字典, 因此为了抗击黑客入侵, 需要为连接用户设置强悍的密码, 让黑客无从破解。为了提高安全性, 最好将PPTP VPN升级到安全性较高的SSL VPN, 为了防止ARP等, 需要在服务器上安装各种安全软件, 配置防火墙规则来保护其安全。



Windows IP 安全策略

▼ 新疆 崔良义

Windows IP 策略，是 Windows 自带的一种安全 IP 策略方法。通过相应的策略设置，可以实现阻止和允许访问相关的端口和 IP 地址，相当于拥有了一个免费但功能更加完善的防火墙。

第一步，进入 Windows IP 安全策略界面，点击开始—控制面板—管理工具—本地安全策略，或者开始—运行—输入 secpol.msc。

第二步，创建一个 IP 安全策略名。选中左侧导航树中“IP 安全策略，在本地计算机”，右键选择“创建 IP 安全策略”，或者在命令行窗口下输入 netsh ipsec static add policy name=myname，其中 myname 指 IP 策略名。

第三步，创建 IP 筛选器列表和筛选器操作。选中左侧导航树中“IP 安全策略，在本地计算机”，右键选择“管理 IP 筛选器列表和筛选器操作”，创建一个名为 denyAll 的 IP 筛选器列表，在 IP 筛选器属性中，目标地址应选择“我的 IP 地址”，“镜像”左边的钩去掉，其他默认；创建一个名为 deny 的筛选器操作，新筛选器操作属性中，选择“阻止”。

第四步，添加规则。双击 IP 安全策略名，单击“添加”，在“新规则属性”对话框中，“IP 筛选器列表”标签中选择刚建立的 denyAll，“筛选器操作”标签中选择刚建立的 deny，这样就创建了一个阻止所有端口、所有 IP 地址的安全策略。

第五步，创建允许访问的 IP 筛选器列表和筛选器操作。根据第三步方法，创建一个名为 permit 的 IP 筛选器列表，并添加相应允许访问的 IP 地址，新筛选器操作属性中，选择“许可”。同理，根据第四步方法添加相应规则，这样就创建了一个允许用户访问的安全策略。

第六步，指派安全策略。Windows IP 策略默认是不指派的，选中 IP 策略名称，右键选择“分配”，此时，该策略名称上多了一个小绿点，表示策略启用成功。

在第五步添加相应允许访问的 IP 地址时，根据实际情况，“源地址”可以选择一个特定的 IP 地址，也可以选择一个特定的 IP 子网，还可以选择一个特定的 DNS 名称。另外，在“协议”标签中还可以设置具体允许访问的协议和端口，如选择协议类型为 TCP，设置 IP 协议端口从任意端口到此端口，填写 3389，则对应 IP 地址仅能访问该服务器远程端口。

Windows IP 策略应用场景非常广泛，如对于某些重要的 Web 服务器，我们只希望某些特定用户允许访问，只需将其固定 IP 地址加入其服务器 IP 策略即可；对于某些重要的数据库服务器，屏蔽其他 IP 地址及数据库端口（管理员除外），这样用户即使拥有数据库密码也无法访问数据库；通过以上方法设置 Windows IP 安全策略，服务器就多了一道屏障，数据就多了一份安全。

❖ 移动设备安全靠策略

▼ 江苏 孙秀洪

停用自动播放功能

Windows 系统自动播放移动设备窗口内容的特性，常常会被恶意病毒利用，成为病毒自动发作运行的良好载体。为了不让移动设备成为病毒木马传播的温床，立即停用 Windows 系统自动播放移动设备的功能，是相当有必要的。在停用自动播放功能时，不妨进行如下设置操作：

首先，在移动设备待插计算机系统中，逐一点击“开始”、“运行”命令，展开系统运行对话框，输入“gpedit.msc”命令并回车，开启系统组策略编辑器运行状态，在组策略编辑窗口左侧列表中，将鼠标定位到“本地计算机策略”、“计算机配置”、“管理模板”、“系统”节点上，从目标节点下面选中“关闭自动播放”组策略，打开该选项的右键菜单，点击“属性”命令，切换到如图 1 所示的组策略属性对话框。

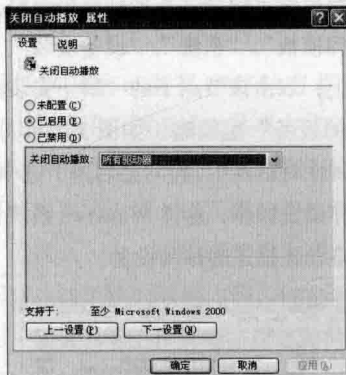


图 1 组策略属性对话框

检查这里的“已启用”选项是否已被选中，如果发现其没有被选中时，应该及时将其重新选中，再从“关闭自动播放”位置处选中“所有驱动器”选项，确认后保存设置操作。

这样，日后任何移动设备插入到本地计算机后，Windows 系统都不会自动播放其中的内容了，这时潜藏在移动设备中的病毒木马也就无法发作攻击本地系统或

网络了，除非用户自己双击移动设备图标，网络病毒才会有机会激活运行。

注意

当然，这种方法停用移动设备自动播放功能比较极端，它会对光盘的自动播放带来影响。

按需分配操作权限

在移动设备随处可见的今天，网络环境中的很多隐私数据往往会被移动设备顺带“捎走”。为了预防这种现象发生，很多人会通过 BIOS 设置简单封死计算机主板上的 USB 接口，但这也意味着合法用户也无法使用移动设备保存数据。其实，我们可以进行适当设置操作，为不同级别的用户设置不同的移动设备操作权限。例如，要想让“asd”用户可以正常显示移动设备，又可以成功读写其中的内容，让“fgh”用户无法读写移动设备中的内容时，只要进行下面的设置操作：

首先，依次单击“开始”、“运行”命令，弹出系统运行对话框，输入“notepad.exe”命令，启动运行记事本应用程序，创建一个让“asd”用户可以正常显示移动设备，又可以成功读写其中内容的批处理文件，假设该文件名称为“asd.bat”，在该文件编辑窗口中输入如下命令代码：

```
regadd HKLM\SYSTEM\CurrentControlSet\Services\
USBSTOR/v Start/t Reg_Dword/d 00000003/f
```

```
regadd HKLM\SYSTEM\CurrentControlSet\Control\
StorageDevicePolicies/v WriteProtect/t Reg_Dword/d
00000000/f
```

这里的第一行代码表示可以查看移动设备分区窗口，第二行代码表示可以向移动设备读取和写入数据。

同样地，再创建一个让 fgh”用户无法读写移动设备内容的批处理文件。接着，以“asd”用户账号登录

计算机,依次单击“开始”、“运行”命令,弹出系统运行对话框,输入“gpedit.msc”命令,打开系统组策略编辑窗口,在该窗口的左侧列表中,将鼠标定位到“本地计算机策略”、“计算机配置”、“Windows 设置”、“脚本(启动/关机)”节点上,选中该节点下的“启动”组策略,并用鼠标双击之,展开如图 2 所示的组策略属性对话框。点击“添加”按钮,将之前创建好的、能正常显示移动设备又能成功读写其内容的“asd.bat”批处理文件添加进来,确认后返回。日后,“asd”用户每次成功登录计算机系统时,都会自动调用“asd.bat”批处理文件,这样“asd”用户既能查看移动设备窗口内容,又能对其中的内容进行读写操作。



图 2 组策略属性对话框

换成“fgh”用户账号登录本地计算机系统,开启系统组策略编辑器运行状态,逐一展开“本地计算机策略”、“计算机配置”、“Windows 设置”、“脚本(启动/关机)”节点,双击该节点下的“启动”组策略,在其中导入之前创建好的“fgh.bat”批处理文件,单击“确定”按钮执行设置保存操作。日后,“fgh”用户每次登录进入本地计算机后,都会自动调用“fgh.bat”批处理文件,这样本地计算机中的 USB 接口会被禁止使用,那么“fgh”用户此时插入移动设备,也无法使用它带走本地计算机中的隐私数据。

安装特定移动设备

大家知道,简单地限制计算机主板上的 USB 接口,会影响计算机主人使用移动设备。为了既能限制别人使用移动设备,又不影响用户自己使用移动设备,我们能否让 Windows 系统变得更智能一些,仅允许安装用户主人的移动设备,而不允许安装其他移动设备呢?答案是肯定的!在 Windows 7 系统环境下,我们就能使用相对“温和”的方法,仅允许 Windows 系统安装特定用户的

移动设备。

例如,现在想让 Windows 7 系统只安装笔者自己的移动硬盘设备,而禁用其他移动设备,要做到这一点,可以先将自己的移动设备插入到计算机主板上的 USB 接口中,让 Windows 系统能够正常识别并访问它,之后依次单击“开始”、“控制面板”命令,弹出系统控制面板窗口,用鼠标双击其中的“设备管理器”图标,从设备管理器界面中展开“便携设备”分支,找到自己的移动硬盘设备。

用鼠标右键单击移动硬盘设备图标,点击右键菜单中的“属性”命令,展开移动硬盘属性对话框,选择“详细信息”选项卡,在对应选项设置页面的“属性”位置处,选中“硬件 ID”选项,这时在“值”位置处会出现一个字符串,它就是笔者所用移动硬盘的设备 ID,将该数值记忆下来,接着返回到设备管理器窗口,展开“通用串行总线控制器”节点,选中该节点下的“USB 大容量存储设备”选项,打开该选项的右键菜单,点击“属性”命令,选择该设备属性框中的“详细信息”选项卡,在对应选项设置页面的“属性”位置处,选中“硬件 ID”选项,同时将该选项的数值也记忆下来。

找到笔者所用移动设备的硬件 ID 后,现在就能使用组策略实现限制安装设备目的了。依次单击“开始”、“运行”命令,弹出系统运行对话框,输入“gpedit.msc”命令,打开系统组策略编辑窗口,在该窗口的左侧列表中,将鼠标定位到“本地计算机策略”、“计算机配置”、“管理模板”、“系统”、“设备安装”、“设备安装限制”节点上,双击该节点下的“禁止安装未由其他策略设置描述的设备”组策略(如图 3 所示),在其后出现的组策略属性对话框中,将“已启用”选中,单击“确定”按钮保存设置操作,这样 Windows 系统日后会自动禁止安装策略设置描述的移动设备。



图 3 “禁止安装未由其他策略设置描述的设备”组策略

之后,再次将鼠标定位到“本地计算机策略”、“计算机配置”、“管理模板”、“系统”、“设备安装”、“设备

安装限制”节点上,找到该节点下的“允许安装与下列设备 ID 相匹配的设备”组策略,并用鼠标双击之,在其后弹出的设置界面中,将之前记忆下来的合法设备 ID 导入进来,确认后保存设置操作。

注意

这样,Windows 系统日后就能智能识别笔者的移动硬盘设备,而不会安装其他移动设备了。

禁用自动运行命令

一些病毒木马之所以能够通过移动设备,轻易威胁网络或数据安全,主要是在该设备上悄悄写入了能够自动运行的恶意程序。在 Windows 7 系统环境下,我们可

以通过合适设置,禁止 Windows 系统运行移动设备上的所有自启动命令,那么病毒木马也就无法将移动设备当成传播载体了。

依次单击“开始”、“运行”命令,弹出系统运行对话框,输入“gpedit.msc”命令,打开系统组策略编辑窗口,在该窗口的左侧列表中,将鼠标定位到“本地计算机策略”、“计算机配置”、“管理模板”、“Windows 组件”、“自动播放策略”节点上。

其次找到该节点下的“自动运行的默认行为”选项,打开该选项的右键菜单,点击“属性”命令,切换到对应选项设置对话框,选中“已启用”选项,同时选中“不执行任何自动运行命令”选项,单击“确定”按钮结束设置操作。这样,Windows 7 系统日后就能禁止运行移动设备上的所有自启动命令。

安全“例外”效率兼顾

江苏 王根宏

隔离“例外”让共享高效

单位局域网某台计算机中存储有非常重要的数据,为了防止普通用户随意通过共享方式,偷窥到单位的隐私内容,网络管理员在这台计算机系统中启用了 Windows 系统内置防火墙,以实现与其他终端计算机的软式隔离。但这么一来,单位领导就无法通过网络共享方式,访问到这些重要的数据内容,每次到重要计算机现场去访问,又会影响工作效率,这该如何是好呢?

很简单!巧妙利用 Windows 系统防火墙的“例外”功能,就可以仅让单位领导的计算机能够共享访问重要计算机系统,而其他计算机则无权访问。以系统管理员登录进入重要计算机系统,依次单击“开始”、“设置”、“控制面板”命令,弹出系统控制面板窗口,双击其中的“Windows 防火墙”图标,展开系统防火墙配置对话框。选择“常规”标签,选中该标签设置页面中的“启用”选项,开启防火墙的运行状态。之后点选“例外”标签,选中该标签页面中的“文件和打印共享”复选项,单击“编

辑”按钮,切换到编辑服务设置框中,将“TCP 139”、“TCP 445”、“UDP 137”、“UDP 138”等端口选项同时选中,再按下“更改范围”按钮,进入如图 1 所示的设置界面。选中“自定义列表”选项,在对应选项文本框中,输入单位领导计算机的 IP 地址,如果要输入多台计算机地址,必须要注意每个地址之间用逗号隔开,同时添加子网掩码 255.255.255.0 地址。例如,可以输入“10.176.0.131, 10.176.0.132, 10.176.0.133, 10.176.0.134/255.255.255.0”,单击“确定”按钮保存设置操作。

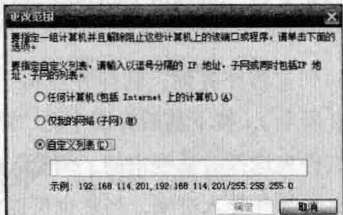


图 1 选择“自定义列表”

注意

这个时候，因为局域网中的其他计算机受到了防火墙软式隔离，将不能正常共享访问那台保存有重要数据的新计算机了，但是具有防火墙例外功能的领导计算机是能够访问到它的。

虚拟“例外”让升级高效

为了防范病毒木马的攻击，不少用户安装使用了虚拟系统，这样日后遭遇到的病毒木马不管破坏性有多么强大（例如修改 IE 浏览器设置、偷偷创建陌生帐户等），只要简单地重新启动计算机系统，所有破坏性操作都会被强制还原，Windows 系统的工作状态也将毫发无损。

注意

然而，虚拟系统常常一股脑地将所有发生变化的数据自动删除掉，对安全工具的升级数据也会毫不手软，这显然会影响杀毒软件的升级效率。

为了既能保护 Windows 系统的工作状态，又能不影响杀毒软件的病毒更新效率，我们可以利用一些虚拟系统的“例外”功能，将杀毒软件的病毒库更新文件夹排除在安全保护之外，让特定位置能够正常存储数据，这就相当于在虚拟系统中打开一扇“暗门”，从而很好地解决病毒库及时更新问题。

例如，在“Shadow Defender”虚拟系统环境下，我们可以利用它的“例外列表”功能，来存储病毒库所在的文件夹，让还原操作不影响到病毒更新操作。首先退出虚拟系统状态，让计算机系统进入正常工作状态，在该状态下打开“Shadow Defender”程序主操作界面，单击“模式设置”按钮，进入模式设置页面，选中该页面中的所有磁盘分区，点击“启动影子模式”按钮，让所有磁盘分区都能受到“Shadow Defender”工具的还原保护。

接着返回到主程序界面，选择并点击“例外列表”选项（如图 2 所示），按下其后界面中的“添加文件夹”按钮，点击文件夹选择对话框中的“浏览”按钮，将病毒库的文件夹选择并导入进来，当然也可以将其他需要排除在安全保护之外的文件夹添加进来，确认后执行重新启动操作，强制系统进入虚拟系统状态。

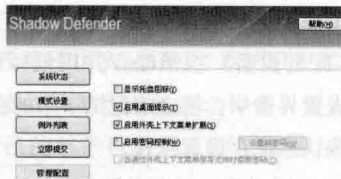


图 2 例外列表选项

注意

这时候，在该状态下执行病毒库更新操作时，升级数据就不会被虚拟系统自动删除了。

遇到某些虚拟系统没有“例外”功能时，不妨将一些重要文件夹转移到系统分区之外，因为虚拟系统一般保护的多是系统分区。在日常办公过程中，有些用户经常喜欢将工作文档存储到“我的文档”、“桌面”等系统文件夹中，要将这类文件夹转移到系统分区以外的位置时，可以依次单击“开始”、“运行”命令，弹出系统运行对话框，输入“regedit.exe”命令并回车，开启系统注册表编辑器运行状态。在该窗口的左侧列表中，将鼠标定位到“HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Explorer\Shell Folders”注册表节点上，如图 3 所示。找到目标节点下与“我的文档”、“桌面”等系统文件夹有关的项目，将它们重新指向其他的磁盘分区即可。



图 3 注册表编辑器

注意

如果计算机安装使用的是 Windows 7 系统，那么也可以直接打开特定文件夹的右键菜单，点击其中的“属性”命令，进入对应文件夹属性对话框，在其中修改该文件夹的分区路径即可。

扫描“例外”让杀毒高效

对付那些悄悄藏匿于移动硬盘或优盘中的自启动类型病毒,最有效、最快捷的应对办法,就是使用版本最新的杀毒程序,智能扫描移动设备中的数据文件,保证这些设备中的自启动类型病毒在没有发作之前,已经被强制清除干净。

注意

只是,大家平常使用的移动设备分区很可能多是没有病毒的,如果让杀毒程序每次自动扫描用户自己的移动设备,需要耗费很长时间,显然这会影响到系统的杀毒效率。

其实,通过正确定义杀毒程序有关参数,仅让其自动扫描陌生用户的移动设备分区,既能有效预防藏身于陌生移动设备中的自启动类病毒,又能大大提升杀毒软件的查杀效率。

例如,笔者自己的计算机系统中事先已安装了NOD32杀毒程序,要想让该杀毒程序自动扫描陌生用户使用的移动设备分区,而不扫描自己的移动设备分区时,可以先打开对应杀毒程序界面中的“ESET Smart Security”设置框,在“文件系统实时防护”位置处,点击“高级设置”按钮,切换到杀毒程序高级设置对话框,之后按下“可移动磁盘上的文件时采用高级启发式扫描”处的“例外”按钮,弹出文件夹浏览对话框,从中将移动设备所使用的磁盘分区符号逐一选中并导入进来。经过之前的设置操作,平时频繁使用的移动设备插入到本地计算机系统后,杀毒程序是不会对它进行扫描查杀的,而有陌生用户的移动设备插入到本地计算机系统时,杀毒程序就会对它自动扫描查杀了,这样就能很高效地预防自启动类型病毒程序的恶意攻击了。

阻断“例外”让浏览高效

大家知道,通过 Windows 系统的软件限制策略,可以轻松阻断已知文件名称类型病毒的运行,但这种阻断操作容易影响一些正常程序的运行,例如一些“iexp*.exe”类型的病毒,与 IE 浏览器的应用程序名称“iexplorer.exe”十分相近,如果简单地利用软件限制策略,定义“iexp*.exe”程序不能自动运行的策略时,就会同时阻断 IE 浏览器程序的运行,从而影响到用户的正常上网浏览操作。

要想在成功阻断病毒的前提下,让上网浏览更高效,可以在自定义特定程序不允许自动运行的情况下,通过创建新散列规则来对特殊类型的文件实现阻断“例外”。例如,要阻断“iexplorer”病毒程序自动运行时,可以依次单击“开始”、“运行”选项,展开系统运行对话框,输入“gpedit.msc”命令并回车,开启系统组策略编辑器运行状态。在该编辑窗口左侧显示列表中,逐一展开“本地计算机策略”、“计算机配置”、“Windows 设置”、“安全设置”、“软件限制策略”选项,在目标选项下面新建路径规则,在其后弹出的新建路径对话框中,将路径设置为“iexp*.exe”,从安全级别下拉列表中选择“不允许”,确认后执行设置保存操作。

注意

这个时候,启动运行 IE 浏览器程序时,系统会弹出禁止运行的提示,这说明之前设置的路径规则已经生效,因为 IE 浏览器程序名称为“iexplorer.exe”,所以该程序会被强行禁止运行。

为了能让 IE 浏览器程序不受影响,我们还需要定义散列规则,让正常的浏览器程序排除在阻断列表之外。在进行这种定义操作时,先返回到如图 4 所示的“其他规则”子项上,打开它的右键菜单,单击“新散列规则”命令,切换到散列规则创建对话框,按下“浏览”按钮将“iexplorer.exe”导入进来,同时从安全级别下拉列表中选择“不受限制”选项,单击“确定”按钮保存设置操作,这样就能实现阻断“例外”让上网浏览更高效目的了。

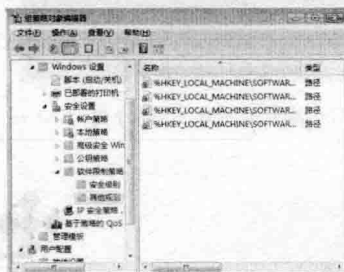


图4“其他规则”子项

拦截“例外”让运行高效

恶意用户成功发动溢出攻击,同时窃取计算机或服务系统 shell 后,或许会执行类似“regedit.exe”、“del.exe”这样危险的命令或程序,来对 Windows 系统实施

进一步的非法攻击。为了防止这样的攻击，很多人会简单启用计算机系统的“阻止访问命令提示符”组策略，来禁止用户在 DOS 命令行窗口执行所有程序命令。

注意

很明显，这种拦截方法会影响一些日常办公程序的运行。为了既能拦截危险命令程序，又能保证正常工作程序的高效运行，我们可以按照如下步骤，实现拦截“例外”效果。

首先依次点击“开始”、“运行”选项，在弹出的系统运行对话框中，输入“gpedit.msc”命令开启系统组策略编辑器运行状态。将鼠标定位到该编辑窗口左侧列表中的“本地计算机策略”、“用户配置”、“管理模板”、“系统”节点上，用鼠标双击该节点下的“只运行许可的 Windows 应用程序”选项，打开如图 5 所示的组策略属性对话框，选中“已启用”选项，激活并点下“显示”按钮，在其后界面中将那些合法的工作程序添加导入进来。



图 5 组策略属性对话框

接着将鼠标定位到“本地计算机策略”、“用户配置”、“管理模板”、“系统”节点上，找到并用鼠标双击指定节点下的“阻止访问命令提示符”组策略，进入对应组策略属性对话框，选中“已启用”选项，单击“确定”按钮后，就能禁止用户在 DOS 命令行窗口执行一些危险的程序或命令了。

此外，从 Vista 系统开始，UAC 功能一直在为用户提供安全拦截功能，但该功能也会给用户带来麻烦：有些经常使用的程序，明明知道是安全的，可每次运行它时，UAC 功能总会重复弹出拦截提示，让人感觉到十分不爽。

为了实现拦截“例外”效果，我们可以通过“UAC Trust Shortcut”这款工具，来为安全的程序创建特殊快捷方式，日后通过双击快捷图标方式，就能跳过 UAC 功能的安全拦截了。开启“UAC Trust Shortcut”程序的运行状态，在“Name”位置处输入安全程序的快捷图标名称，按下“Browse”按钮，弹出文件选择对话框，选中并添加安全程序文件，之后点击“Add Now”按钮。这个时候，就会在系统桌面上自动创建好对应程序的新快捷图标，日后通过该图标，就能跳过 UAC 功能的安全拦截，实现高效启动运行目的了，操作也十分简单。

重识“DNS 劫持”

武汉 袁斯坦 刘辉

为了提高工程档案的利用率，公司决定对档案这边库存的工程底图进行数字化，数字化后的电子图会挂接到扫描图管理系统中，以便设计人员查询和利用。在使

用这个扫描图管理系统的过程中，我们选用了 360 安全浏览器，结果在使用系统的在线浏览功能进行前后翻页的时候，出现了浏览器会自动跳转到某个特定的体育网

站(310pe.com)的情况。但用杀毒软件对服务器和客户端进行查杀,并未发现任何木马或病毒,对系统源代码进行检查,也未发现植入了那个体育网站。最后通过修改服务器和客户端的 Host 文件后,问题才得到完美解决。

当这次事件发生时,本以为是和“DNS 劫持”有关,于是选择了对付“DNS 劫持”的方法,但效果很不理想,反反复复多次后,还是无法彻底解决。最后,笔者查阅了相关资料才发现,此事件实际上是一次“DNS 污染”,而非“DNS 劫持”。

什么是 DNS

DNS 是计算机域名系统或域名解析服务器(Domain Name Server 或 Domain Name System)的缩写。

DNS 的作用打个比方说:当你在地址栏输入 www.baidu.com 时,电脑不是直接就连接到百度服务器里的,而是先向 DNS 服务器查询 www.baidu.com 的 IP 地址,然后再按照这个 IP 地址转到百度的服务器里。一般每个地区都会有一个特定的 DNS 服务器,是由 ISP 提供的,想知道自己地区 DNS 的话,可以去咨询自己的网络服务提供商。

什么是 DNS 劫持

DNS 劫持就是通过某些手段取得某域名的解析记录控制权,进而修改此域名的解析结果,导致对该域名的访问由原 IP 地址转入到修改后的指定 IP,其结果就是对特定的网址不能访问或访问的是假网址,从而实现窃取资料或者破坏原有正常服务的目的。

DNS 劫持通过篡改 DNS 服务器上的数据、返回给用户一个错误的查询结果来实现。

DNS 被劫持后的表现有很多,例如:打开正常网站的时候,会莫名出现一些弹窗广告;点击下载链接,下载的并不是所需要的东西;浏览器输入一个网址后回车网页跳转到其他网址的页面。这样的网址,有时甚至会劫持购物网站的链接,导致打开虚假网站,泄露个人隐私、威胁个人财产安全等。

什么是 DNS 污染

DNS 污染是一种让用户由于得到虚假目标主机 IP

而导致不能与真正主机通信的方法,DNS 受污染的途径主要有两种:

一是攻击者监测到 DNS 查询的请求报文时,伪装成 DNS 服务器向发出请求主机发送响应报文。因为 DNS 报文通常是无连接的 UDP 报文,没有确认机制,源主机不能识别出这个报文并非出自 DNS 服务器。攻击者并不需要丢弃真正 DNS 服务器发回来的响应报文,因为 DNS 的机制会导致源主机只接受最先到达的响应报文(甚至不管是谁发的)而忽略后继到达的其他报文。这样,源主机得到的就是攻击者伪造的域名解析结果。DNS 污染是发生在用户请求的第一步上,直接从协议上对用户的 DNS 请求进行干扰。目前一些被禁止访问的网站很多就是通过 DNS 污染来实现的。

二是本地 DNS 服务器的缓存已受到污染,里面缓存的是错误的结果。DNS 服务器通常将 DNS 查询的结果缓存在本地一段时间,这本意是为了减少重复 DNS 查询,从而降低 DNS 报文占用的网络带宽,可如果某次 DNS 查询的结果受到污染,则后继一段时间内向该 DNS 服务器查询的结果都会受到污染。

我们可以在命令行下,通过下面这样的命令来验证是否受到了“DNS 污染”:nslookup 144.223.234.234,即可判断该域名是否被污染,由于 144.223.234.234 不存在,理应没有任何返回,如图 1 所示。但如果我们得到了一个错误的 IP(不确定),即可证明已经被 DNS 污染了。



图 1 正常的 DNS 返回值

解决方法

1. 对于 DNS 劫持,只需要把系统的 DNS 设置手动切换为国外的 DNS 服务器的 IP 地址即可解决。
2. 对于 DNS 污染,可以说,个人用户很难单靠设置解决,通常可以使用 VPN 或者域名远程解析的方法解决,但这大多需要购买付费的 VPN 上网或使用各种 SSH 加密代理进行远程 DNS 解析等。如果你只是某浏览器的用户,又懒得折腾,可以直接打开此浏览器的远

程 DNS 解析就行了。在地址栏中输入：

about:config

找到 network.proxy.socks_remote_dns 一项改成 true。

当然，我们也可以通过修改 Hosts 的方法来解决。操作系统中 Hosts 文件的权限优先级高于 DNS 服务器，操作系统在访问某个域名时，会先查询 Hosts 文件，然后再查询 DNS 服务器，我们可以在 Hosts 屏蔽受到污染的 DNS 地址来解决 DNS 污染，或手动设置域名对应的正确 IP 地址。

其中几个 Hosts 里可屏蔽的地址，复制到本地的 host 文件（如 Windows 7 X64 中，Host 文件路径为

“C:\Windows\System32\drivers\etc”）保存即可。

写在最后

“DNS 劫持”和“DNS 污染”，在我们的日常工作、生活中都可能会遇到。由于“两兄弟”长得比较像，我们很容易弄混淆，在进行处理的时候容易犯“张冠李戴”的错误，时间耗费了、问题却没解决。通过本文的探讨，希望能让大家重新认识它们，并选择合适的方法来解决问题。

包过滤保障网络安全

山东 何钰 李瑞祥

面对互联网和内部网络的复杂环境，网络的安全越来越受到运维人员的重视。笔者单位的 Radius 系统承担着宽带用户计费 and 认证等重要责任，它的安全不容忽视。为更好的服务用户，提高其上网体验。计划实现宽带到期提醒。针对该功能的实现并考虑到 Radius 设备安全，本文就如何实现 Radius 和强推服务器的共存，并实现强推功能等问题展开讨论。最终通过使用路由和包过滤策略具体实现了网络需求。

强推服务器主要来解决用户到期提醒的问题，其工作原理是用户到期后可以正常拨号，但不同的是 Radius 会回复 BRAS 信息，该用户已经到期。根据这个信息 BRAS 会将该到期用户正常上网行为限制。而且利用服务器 Web 强推功能，在用户浏览网页的时候，会强制转到一个服务器设置好的页面，在该页面上会出现用户到期等相关内容。接下来依据其原理根据网络拓扑结构进行服务器和硬件服务器的部署。具体的网络拓扑结构如图 1 所示。

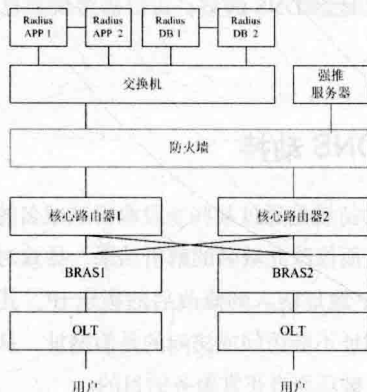


图 1 网络拓扑结构

图 1 中可以看到强推服务器计划部署在新增硬件防火墙的内侧，和强推服务器并列的还有 Radius 服务器集群。当前要实现的网络需求是互联网用户能正常访问强推服务器，但是不能访问 Radius 服务器；同时 Radius 还要和 BRAS 通讯。得知这一具体的网络需求，接下来计划使用路由来实现宽带用户和强推服务器、Radius 和 BRAS 的通讯。具体的配置分别在核心路由器和防火墙上实现。两台核心路由器上配置命令即：

```
interface gei-0/15/0/5
```

```
// 进入核心路由器 1 接口
```

```

description DP-Radius
// 添加描述
ip address 172.28.0.49 255.255.255.252
// 定义连接防火墙接口 IP 地址
interface gei-0/3/0/17
// 进入核心路由器 2 接口
description DP-Radius
// 添加描述
ip address 172.28.0.53 255.255.255.252
// 定义防火墙接口 IP 地址
ip route 10.253.141.0 255.255.255.224 gei-0/15/0/5
172.28.0.50
// 在核心路由器 1 上设置静态路由，并定义出接口
和下一跳 IP 地址
ip route 10.253.141.0 255.255.255.224 gei-0/3/0/17
172.28.0.54
// 在核心路由器 2 上设置静态路由，并定义出接口
和下一跳 IP 地址

```

以上完成了在两台核心路由器端口互联地址和静态路由的设置。紧接着在核心路由器 BGP 路由中重分发静态和直连路由即可，然后将 Radius 服务器的网关设置在防火墙上，最后在防火墙上设置两条等价的默认路由指向核心路由器就可以以实现 BRAS 和 Radius 的正常通信。当然在这里防火墙端口以及 Radius 集群使用交换机的配置命令就不再一一介绍。

回到文章开头的网络需求，引进用户到期提醒强推功能后，用户强推是以 Web 的形式体现，用户可以根据强推服务器的地址进而攻击 Radius 系统，从而威胁到网络的安全性，这就是需要在 Radius 系统与用户、强推服务器之间新增一台防火墙的重要原因，防火墙主要满足以下三点要求：一是强推服务器只与宽带用户通讯，而且强推服务器使用虚拟机实现，方便用户攻击后通过镜像快速恢复强推功能；二是核心路由器与 Radius 之间互相通讯；三是只有网管人员方可登录 Radius 系统。刚才在核心路由器和防火墙上进行静态路由的配置，可以实现互联网用户和强推服务器、Radius 和 BRAS 的通讯，这样虽然实现了网络需求，但是为了保障 Radius 服务的

安全，这就需要配置策略来拒绝互联网用户访问 Radius 的请求，这里就需要使用到包过滤技术。

包过滤技术主要是通过在网络层截获网络数据包，再根据防火墙的规则表来检测攻击行为，并通过对网络层对数据包进行分析、选择。通过检查数据流中每一个数据包的源 IP 地址、目的 IP 地址、源端口号、目的端口号、协议类型等因素或它们的组合来确定是否允许该数据包通过。下面就开始在防火墙上进行包过滤的配置，具体的配置如图 2 所示。



图 2 防火墙包过滤配置示意图

通过图 2 可以看到定义的发起方源 IP 即宽带用户，发起方目的 IP 即 Radius 服务器地址，执行的动作是丢弃，然后启用该策略即可。该策略的作用是将宽带用户访问 Radius 服务器的请求执行丢弃动作，从而在一定程度上提高了 Radius 服务器集群的安全性。完成该包过滤策略的设置后，紧接着删除防火墙设置的指向两台核心路由器的默认路由，取而代之的是增加明细路由回环至核心路由器，这里明细路由的目的地址包括互联网用户、BRAS 的 Loopback 地址以及运维人员网管 IP 地址，这样再结合防火墙上配置的包过滤策略一起使用就可以实现网络的需求。完成这一系列配置后，在使用宽带用户上网环境来访问 Radius 服务器结果是不能成功的，而访问强推服务器是没有问题的。这样就实现了宽带用户可以访问强推服务器，但是拒绝其访问 Radius 服务器的请求，同时还严格限制了访问 Radius 服务器的群体的三项网络需求。

综上所述，通过对网络需求的分析，根据现有网络状况因地制宜的增加硬件防火墙来实现需求，在此过程中首先使用路由将网络进行联通，然后使用包过滤策略进行限制，从而达到了网络的需求。也在一定程度上提高了核心服务器集群的安全系数。

避免单位网络单点风险

浙江 方小明

笔者单位在经过信息系统改造建设后，内外网主要区域及链路已具备了高可靠性与冗余能力。但目前随着某些业务信息化发展的深入进行，业务种类陆续增加、业务规模逐渐扩大，来自内部、外部的业务访问日益增多增广，都使得信息系统中网络通讯这个基础平台的重要性日益突出。本文主要从技术角度出发，就如何使单位信息安全建设跟上整体网络建设的步伐，分析单位信息安全建设总现状、网络与信息安全建设存在的问题，提升网络与信息安全建设的解决方法及意义等方面对网络信息安全建设进行思考。

网络信息安全建设总现状

1. 内网建设情况

内网建设情况如图 1 所示。

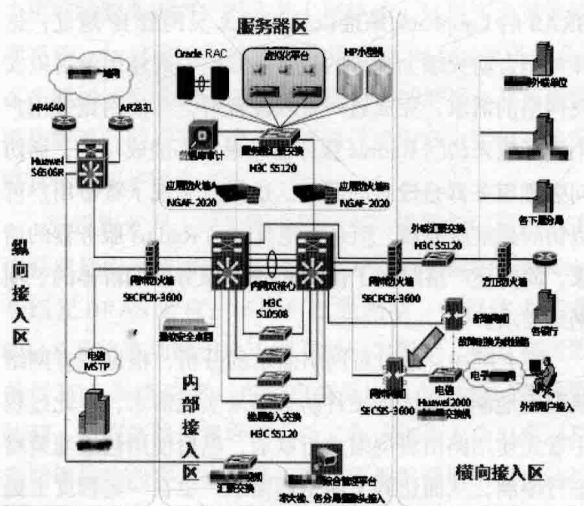


图 1 单位内网架构

笔者单位的信息系统网络由两台互备的 H3C S10508 三层核心交换机提供各区域间的连接，其余各区域如下：

横向接入区，主要与其他外联单位连接，以及各机构对应用系统进行业务访问。

纵向接入区，与上级部门进行连接的区域，通过

S6506R 与 AR4640、AR2831 路由器经由广域网链路，是当前业务、视频会议、管理系统及其视频监控的承载线路。

服务器区域，主要为单位各种业务应用系统，现建有 VMware vSphere 5.5 虚拟化平台、Oracle 数据库实时应用集群、PC 服务器 10 余台、HP 小型机两台，通过一台 H3C S5120 汇聚交换机经由两台应用防火墙连接到核心交换机。

内部接入区，主要为各楼层办公终端、视频监控接入的接入层区域，各楼层通过接入交换机经光纤链路连接到核心交换机。

2. 外网建设情况

楼层终端用户访问 Internet 先经由楼层 H3C S5120 接入层交换机，通过光纤链路上行汇聚至 H3C S10508 外网核心交换机，经由一台天融信防火墙进行地址转换后接入 Internet，并通过一台网络督察设备，对内网的 Internet 访问进行管理与审计。

当前单位信息系统外网拓扑如图 2 所示。

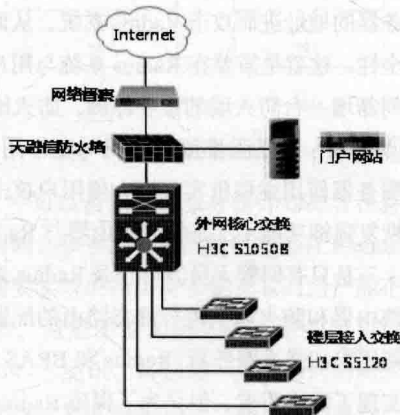


图 2 单位外网架构

3. 链路已初具冗余结构。

单位内外网主要区域及链路基本具备了冗余结构设计，包括内网核心交换的热备、至服务器区域、外联区

域汇聚交换、楼层接入交换的双链路冗余结构,外网核心部分也采用了置备设备进行冷备份,可基本保障楼层终端接入经核心网络到内部服务器的内部网络结构的高可用性要求。

4. 关键设备还存在单点故障。

现阶段单位在网络平台中逐步暴露出一些问题和不足,主要表现为:部分关键通讯节点上,存在着一定的单点故障风险,即当设备需要维护或者出现故障时,缺乏应急措施的设备,网络通讯较难在短时间内恢复正常,导致业务系统的稳定性、连续性无法得到很好的保障。

5. 信息系统安全等级保护未评测。

信息系统的等级保护测评是由具有检验技术能力和政府授权资格的权威机构,依据相关技术规范,按照严格程序对信息系统的安全保障能力进行的综合测试评估活动。通过信息安全等级保护,可以有力地证明单位网络布局、信息系统构建是符合国家有关信息安全等级保护的规定,能证明和提升单位信息安全防范能力。

6. 信息系统数据未实时异地备份。

数据实时异地备份是指在不停止数据库服务的情况下,对数据库进行自动监控,把变化的数据实时地写到异地数据库中,保证数据实时同步。单位目前各类信息系统数据库数据每天晚上进行定时备份,但备份出来的数据主要还是放在机房中的其他服务器上,这就导致虽然有备份,但数据是隔天的且放在机房同一个地方。一旦机房机器硬盘故障、失火等原因会导致数据丢失。

网络信息安全建设不足之处

1. 内网建设单点隐患

外联接入区域单点隐患。横向接入区中外联单位防火墙与汇聚交换机为所有外部通讯接入的“门户”，其重要性较为突出，一旦设备出现故障造成通讯中断而无法迅速恢复正常，将对业务造成严重的影响。

核心路由器单点隐患。当前至广域网的核心路由器华为 S6506R 承载着一些核心应用业务系统,其重要性非常突出,以单位现有条件,暂无可满足替代广域网核心路由器 S6506R 的备选设备,这成为业务系统稳定连续运行的潜在风险隐患。

交换机无应急替换设备。目前单位内网汇聚 / 接入交换机使用情况如下：楼层接 18 台交换机，外联汇聚使用 1 台，服务器汇聚使用 1 台，虚拟化平台使用 1 台，共 21 台。目前数量饱和，并无备用设备可供应急替换

使用,服务器汇聚交换与外联汇聚交换由于分别承载业务系统及外联接入的大量通讯请求,单点故障的风险突出。

2. 外网建设单点隐患。

单位外网出口处部署天融信防火墙,由于年代较长,功能较为简单、防护手段措施相对落后,在面对来自与Internet的各种日新月异的攻击、安全威胁时显得难以应付。加之设备陈旧、性能相对落后,随着单位信息系统规模的扩大,终端数量的增加,已难以处理更高的访问压力请求,同时运行年限的增大,出现故障的风险概率也在与日俱增。一旦设备因为维护、故障造成通讯中断,将导致整个外网通讯完全中断,对业务系统、日常办公造成很大的影响。

网络信息安全提升基本策略

1. 内网信息安全提升策略

针对内网信息安全存在的不足,可以从以下几个方面进行完善,完善后的总体网络拓扑图如图3所示。

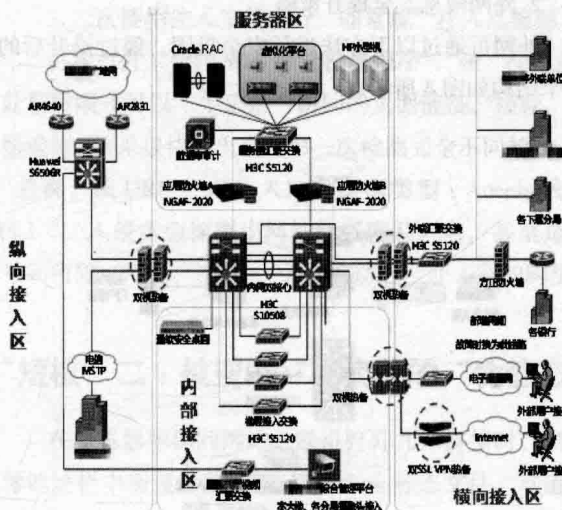


图 3 完善后的内网架构

部署热备网闸。针对当前网络边界隔离的网闸设备单点隐患，新增一台与现有设备功能、型号一致的网闸设备，以热备的方式部署。新增网闸安装在原有设备下，当其中一台设备需要维护或出现故障时，另外一台设备即可动态进入工作，立刻恢复正常通讯，故障修复时间为秒级，以此来保障相关业务的高可用性。

外联防火墙应急策略。当前外联防火墙上承载有所有的外联通讯,部署有相应的地址转换策略,且当前外联区域访问通讯量逐渐增大,现有防火墙设备负载相对

较重,新增一台配置相对高端、性能较高的防火墙作为主防火墙,与其进行热备,共同承担网络边界安全防护的作用。

核心路由器冗余策略。广域网核心路由器 S6506R 作为一个单点故障点,在数据集中之后,承载有整个系统的通信,重要性不言而喻。新增一台能充分满足通讯要求的三层模块化核心交换机,将 S6506R 的现有配置进行导入,并在同一机柜上架,预留线缆以备应急处理、故障切换。以此来保障至广域网出口设备的高可用性要求。

纵向接入区防火墙冗余策略。与外联区域防火墙类似,新增一台防火墙进行热备,共同承担网络边界安全防护的作用。一旦其中一台设备有故障,另一台设备可以马上进入工作。

汇聚/接入交换机应急策略。针对当前交换机数量饱和,无可替代设备作为应急处理预案的现状,新增千兆以太网交换机设备,其中部分作为服务器汇聚交换及外联汇聚交换的热备,剩余不做配置,留作楼层接入、厅视频接入等机动备份。

2. 外网信息安全提升策略

外网可通过以下方法进行安全巩固,经过提升后的整个结构如图 4 所示。

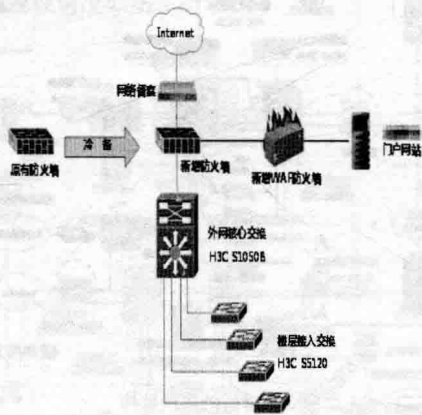


图 4 完善后的外网架构

外网出口功能提升。配置地址转换、访问控制等功能,为单位日常办公访问 Internet 的总出口。

区域防护功能提升。利用应用防火墙先进的应用层级安全防护、网关杀毒等功能为外网访问构筑完善的安

全防护体系。

外网网站服务器防护能力提升。利用应用防火墙的网页防篡改、WebServer 漏洞检测防护等安全防范功能,为单位建设的网站服务器建立防护机制,使其免受攻击威胁。

3. 实施信息安全等级保护

信息安全等级保护主要工作内容包括信息系统定级与备案、安全建设整改、等级保护测评与备案和监督检查,其中信息系统定级与备案和等级保护测评与备案是整个过程中的重要环节。

实施系统定级与备案。信息系统安全保护等级,共分为五个等级,等级越高,所需要实施的保护措施越多越深入。根据对单位信息系统重要程度和信息系统遭到破坏后的危害程度,明确单位信息系统至少要进行两个三级、两个二级的等级保护,且信息系统投入运行后,要提供必要的备案材料。

实施系统测评与备案。在完成信息系统建设和定级工作后,选择符合规定条件的测评机构单位,依据相关技术标准,对信息系统安全等级状况开展等级测评,满足相应等级保护要求。

4. 实施数据实时异地备份。目前,国家对信息安全越来越重视,体现在信息安全技术的应用从个别的行业发展到各行各业,从对电脑设备的重视发展到对核心数据的安全的重视,已是不可逆转的趋势。而单位的计算机应用已非常广泛,而且深入到业务管理的各个环节,系统的数据都存放在服务器的数据库中,实时性要求非常高,所以服务器的备份、数据库的实时备份尤其必要和迫切,解决数据实时异地备份,可避免机房失火,特别是本地机房服务器故障等造成数据的丢失。

构建网络信息安全的意义

可靠的网络信息安全建成后,可以使各部门访问网络系统有可靠的信息安全保障。增加了不法分子通过网络攻击单位的各类应用的难度;增强了各类数据信息的保密性与可靠性;提升了单位对外信息传播及内容的控制能力;提高了网络与信息安全的应急处理能力;保障了单位即使在出现安全问题时可以提供依据。

小心注入式入侵预防中的短板

山东 牟晓东

作为对网站数据库进行入侵攻击的最惯用手段之一,SQL“注入”式入侵攻击因网站模板程序员编写代码时未对用户输入数据的合法性进行严格全面的判断而导致安全隐患的存在。为了预防注入式入侵攻击,很多的网站管理员都会采取一些“防注”措施来阻止入侵者,比如将“and”、“delete”、“;”等敏感注入字符全部列入非法访问的“黑名单”,过滤入侵者所提交的恶意查询字符串;或是通过代码转换的方式将ASP/PHP动态网页转换成“伪静态”的.htm网页,打消入侵者窥探猜解的念头(静态网页没有“注入”漏洞之说)。但这并非万全之策,而且恰恰是这两种自认为较安全的防注入措施有时反倒成为入侵预防中的“短板”!

“短板”一:被“注入中转”注入的“防注”

目前入侵者在检测网站注入点时所使用的工具比较多,其工作流程基本上类似。比如先是将目标网站的某条访问记录的URL进行注入点的常规检测,由于网站管理员事先做过数据库查询命令过滤的“防注”处理,因此在开始检测之后很快就会有提示:“检测失败,该URL不可以进行注入!”(如图1所示)。

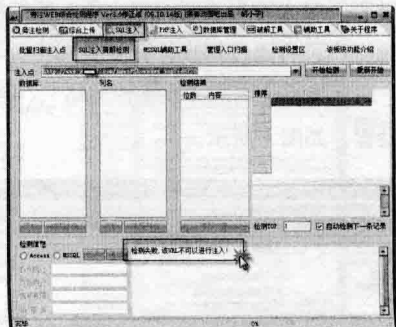


图1 提示检测失败

不过,入侵者为了进一步确认目标网站是否真的不存在入侵的注入点,而不是仅仅依靠工具的机械探测,他可能会在浏览器地址栏该URL记录最后添加一个英

文字符,回车访问后发现“传参错误!参数的值中包含非法字符串!”的提示。这些,都是网站模板中“防注”程序代码的功劳。

1. 借“注入中转生成器”生成有注入点的ASP文件
入侵者用注入中转类工具生成ASP,这样,就得到了一个“.asp”的文件。

2. 搭建好本地ASP运行环境

为给接下来二次使用“旁注Web综合检测程序”注入检测搭好“戏台”——ASP运行环境,入侵者使用工具设置后可在本地计算机浏览器中“半正常”地访问目标网站,说明生成的ASP文件是有效的。

3. 二次使用注入工具进行“非常规”注入点检测

再次打开“旁注Web综合检测程序”,在“注入点”处粘贴刚才可以“半正常”访问的页面链接,接着,开始检测,结果很快就出现与第一次检测完全不同的提示:“恭喜,该URL可以注入!数据库类型:Access数据库!”。入侵者会探测出网站数据库及列名,甚至是账号和密码。可见,“防注”并没有防住“注入”的脚步。

“短板”二:被搜索“出卖”的“伪静态”

在浏览器中访问网站,随机打开几条链接时,浏览器地址栏中所显示的URL都是.htm静态文件,难道这就表示无法被“注入”式入侵所攻击?入侵者有可能尝试使用搜索引擎来查找是否存在动态链接。

1. 工具未查出有注入点但检测到后台登录地址

通过注入工具在“注入连接”后输入URL,接着检测出现提示:“这个连接不能SQL注入!请试别的连接!”。未检测出网站的注入漏洞,但尝试扫描网站的后台登录地址,IE浏览器就可以打开网站链接,就可能进入网站后台管理登录入口。

2. 被模板默认的管理员账号和密码“出卖”

由于之前使用“注入检测”扫描了不存在注入漏洞,

入侵者就无法探测到管理账号和密码，也就无法进行后台登录。但若探测到网站后台管理页面，考虑到很多网站模板系统的默认管理账号和密码都是“admin”之类的简单组合，这就给自己的网站留下了极大的安全隐患！

“短板”修补措施：做好三个“化”

其实，以上两处入侵预防“短板”事例只是网络安全防护漏洞中的冰山一角。在预防“注入”式入侵的防护中，网管员除了要做好最常规的防注入措施外，如网站核心数据库路径及名称的隐藏与防下载、各种危险查询命令字符串的过滤以及一些恶意高频访问 IP 地址自动添加进黑名单等等，还有些比较简单但非常有效的做法：

1. 管理员账号的数目要最少化

大多数网站为了管理的方便而设置了多个管理员账号，而且权限都比较高，这其实是一种比较危险的做法——只要其中一个管理账号被猜解就可能导致整个网

站的沦陷。即使真有设置多个管理账号的需求也应该分出级别，设置好不同的权限，最起码让拥有最高权限的管理账号是惟一的，尽可能减少被注入猜解的几率。

2. 管理登录密码的强度要最大化

虽然密码的强度是个老生常谈的问题，但仍有很多的网站管理员设置使用模板默认密码或是一些简单的密码组合，一旦其对应的 MD5 密码被注入猜解的话，接下来的破解将会变得非常简单。假如管理登录密码足够强大的话，即使是被入侵者注入猜解出 MD5 密码也不能被破解，网站的安全性也可得到一定的保障。建议将自己所设置的密码进行 MD5 加密，然后进行破解测试，如果显示“无法破解”的话就是比较理想的密码。

3. 后台管理登录地址的最隐蔽化

如果不幸被入侵者注入猜解，但只要后台管理登录地址隐蔽得足够好，那也算是比较安全的。因此一定不要使用模板默认的后台路径，更不要在网站首页设置后台管理登录的链接，最好是自定义一个不易被猜解出来的路径名称，以提高其隐蔽性。

构筑信息终端防护“安全之门”

河北 苗增良 刘振军 张伟君

大多数信息系统应用人员可能认为网络安全是网管部门需要关注解决的专业问题，与用户终端关系不大。其实不然，各信息系统终端是企业网络的信息节点，也是关乎信息系统安全的重要环节。为有效防范入侵检测、信息窃取、APT 攻击等安全威胁，做好信息终端防护才能把好“自家大门”，那么平时需要做好的具体工作有哪些呢？就这一问题，笔者结合工作经验做详细介绍。

完善本地安全策略

1. 密码策略设置

严防网络攻击的最基本要求就是配置帐户密码，设置密码时通常要求密码要尽可能复杂，同时合理配置密

码长度最小值、最短使用期限、最长使用期限等策略参数，登录时密码输入错误达到指定次数，系统要能自动锁定该登录帐户，可通过依次打开“管理工具”、“本地安全策略”对话框，依次选择“帐户策略”、“密码策略”选项进行设置，如图 1 所示。

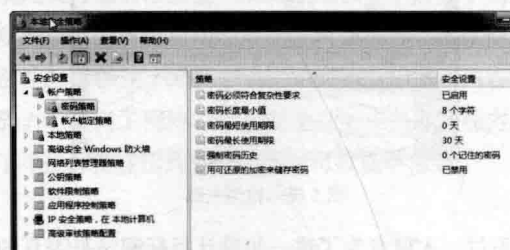


图 1 密码策略设置

2. 审核策略设置

为了保证审核安全信息质量相对提高,减少资源占用率,可通过依次打开“管理工具”、“本地安全策略”对话框,选择“审核策略”选项设置帐户登录、系统事件的审核包含成功和失败操作,策略更改、帐户管理等事件的审核包含成功操作,如图 2 所示。

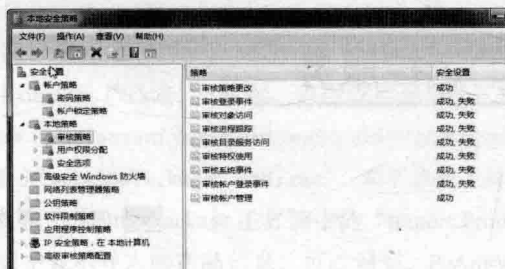


图 2 审核策略设置

3. 用户权限分配

防止默认共享（IPC\$, C\$, ADMIN\$）被用作入侵通道,应严格限制用户的完全控制权限,对威胁系统安全的权限应做到禁用或严格限制,可通过依次打开“管理工具”、“本地安全策略”对话框,选择“用户权限分配”选项进行设置。

优化系统注册表设置

1. 设置注册表修改权限

用户在使用时非常容易忽视注册表,还有许多用户因为怕破坏系统而不敢随意改动注册表,比较安全的做法是仅允许管理员访问注册表,具体方法是,在系统 Windows 目录下找到“regedit.exe”文件,右键选择“权限”选项,将无关用户权限取消,如图 3 所示。



图 3 设置注册表修改权限

2. 清空远程可访问的注册表路径

为有效防止入侵者通过远程访问注册表读取系统信

息,应打开“组策略编辑器”,在“运行”里输入“gpedit.msc”,依次打开“计算机配置”、“Windows 设置”“安全设置”、“本地策略”、“安全选项”,找到“网络访问:可远程访问的注册表路径”选项,将内容全部删除。

3. 修改注册表安全选项

[HKEY_LOCAL_MACHINE] 是系统注册表重要配置,其中存放了系统中各项重要的核心设置数据,只有管理员权限的用户可以访问。然而有许多项通常情况下都是默认设置,如图 4 所示,存在诸多隐患,所以需要修改参数确保系统更加安全。具体步骤是,打开“开始”按钮,点击“运行”,输入“regedit”,打开注册表编辑器,进行以下操作:为防范 ICMP 重定向报文攻击,需改 HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Services\Tcpip\Parameters, 将 EnableICMPRedirects 值由 1 设为 0;为防范 SYN 洪水攻击,需改 HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Services\Tcpip\Parameters, 新建 DWORD 值,名为 SynAttackProtect, 值为 2;为防范 IPC 空连接隐患,需改 HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Control\Lsa, 将 restrictanonymouse 值由 0 设成 1。相关安全设置还有很多,在此省略。

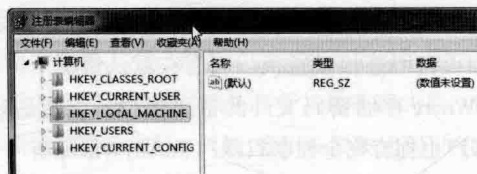


图 4 系统注册表

制定 IP 安全策略

IPSec 支持系列加密算法,可进行数据源认证,筛选特定 IP 或端口,提供安全、透明、高效的网络防护。可在“IP 安全策略”里配置:

1. 定义策略

依次打开“管理工具”、“本地安全设置”对话框,右击“IP 安全策略”选项,选择“创建 IP 安全策略”。

2. 定义筛选器

右键点击“IP 安全策略”选择“管理 IP 筛选器表和筛选器操作”,定义“IP 筛选器列表”和“IP 筛选器属性”,设置“源地址”、“目标地址”、“协议类型”、“协议端口”。

3. 定义规则属性

在“新规则属性”窗口中点选创建的规则,点击“管理筛选器操作”选项卡下的“添加”,选择“安全措施”下的“阻止”选项。

4. 策略生效

在“组策略”窗口中,右击“创建的策略”,选择“分配”选项,启用该策略。

打造更安全的远控服务

河南 郭建伟

在通常情况下,PcAny Where 的安全性存在一些问题,因为其产生的“*.cif”密码文件很容易破解。在很多入侵案例中,黑客往往采取利用网站漏洞,上传 WebShell 木马,之后下载 PcAnyWhere 密码文件。对其破解后,利用获取的密码连接目标主机。黑客甚至在本地安装 PcAnyWhere,之后创建一个“.cif”密码文件,之后利用 WebShell 的文件上传功能,将密码文件直接存放到“C:\Document and Settings\All Users\Application Data\Symantec\pcAnywhere\Hosts”文件夹中,之后使用预设密码连接被控机。因为在默认情况下,对于 PcAnyWhere 存储密码文件的目录来说,即使是 Users 组的账户也拥有完全控制权限! PcAnyWhere 有一个特点,高版本可以兼容低版本,因此,黑客可以很轻松的创建和上传密码文件。

为了抗击黑客对 PcAnyWhere 的威胁,很多网管员会使用系统自带的 IPSEC 安全策略,针对 PcAnyWhere 使用的端口创建安全规则,只允许的 IP 连接被控端主机。或者使用 PcAnyWhere 内置的安全机制,实现对登录地址的识别,进而阻止黑客获得连接密码后发起的攻击行为。但是,上述方法也存在一定的问题,一旦网管员更换了 IP(例如使用 ADSL 方式上网或者是动态 IP 等),就无法连接 PcAnyWhere 被控端了。其实,在 PcAnyWhere 中已经内置了 Serial ID 安全认证机制,可以完美的解决上述问题。让黑客即使知道了连接的用户名和密码,也无法对 PcAnyWhere 主机进行非法控制,而网管员则可以在任意主机上连接 PcAnyWhere 被控端,实现自由的远控操作。

PcAnyWhere 的 Serial ID 安全验证机制的作用就是

限定基本的登录环境,即使用户名和密码被盗,黑客也无法登录到使用了 Serial ID 验证机制的主机上。在被控端按照常规步骤,安装好 PcAnyWhere,在其主界面左侧的“查看”框中点击“转到高级视图”项。切换到高级视图界面,在左侧的“PcAnyWhere 管理器”框中点击“串口表示集合”项,在右侧窗口空白处点击右键,在弹出菜单(如图 1 所示)中点击“新建”→“项目”项,在弹出窗口中的“使用以下串口来限制主机连接”栏中输入 SerialID 号,注意其范围要大于 0 小于 4294967296。如果超出该范围,PcAnyWhere 就弹出序列 ID 值无效的提示。点击添加按钮,将其添加到序号列表中。当然,可以添加多个 Serial ID 号,这些序号不能相同。点击确定按钮,完成 Serial ID 文件的创建操作。如果采用默认安装,其存放路径为“C:\Documents and Settings\All Users\Application Data\Symantec\pcAnywhere\Serial ID Sets”。为了便于使用,最好将其备份起来。

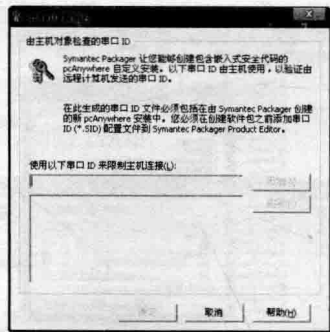


图 1 创建 Serial ID 安全文件

要想发挥 Serial ID 认证的功能,需要使用 Symantec Package 这款工具,来创建特定的 PcAnyWhere 安装包。使用 Symantec Package 这款工具,可以创建,修改自

定义安装包,之后将其发布给所需用户即可。此外,使用该工具还可以创建只包含用户所需功能的设置项目的安装包,这样利用定制适合企业环境的软件环境。当然,也可以使用 Serial ID 验证方式,来限制登录用户的身份。使用 WinMount 等工具打开 PcAnywhere 安装光盘文件,在其中运行“setup.exe”程序,在安装界面中点击“View Other Installation Options”链接,在弹出窗口中点击“Download System Package”链接,下载 Symantec Package 安装包。也可以打开网址“http://www.solutionsam.com/solutions/public/pcAnywhere/v12_5/Packager/Packager_ENG.exe”,来下载该工具。

在 Symantec Package 主界面中的“Import Products”面板中显示导入的产品信息,可以看到, PcAnywhere 已经自动添加进来了。在“Configure Products”面板中双击“Symantec pcAnywhere”项,在弹出窗口中的“Feathers”面板中提供了基本的安装元素,包含了 PcAnywhere 的各个功能选项,允许您对其各项功能进行取舍。一般来说,采用默认设置即可。在“Configuration Files”面板中配置所需文件,在“Install Options”面板中设置安装选项。如果您对 PcAnywhere 非常熟悉,可以根据自己的需要定制以上各个选型。

例如选择“Remote Files (*.CHF)”项,可以添加后缀为“.CHF”的文件,该文件是主控端连接被控端的配置文件。选择“Host Files (*.BHF)”项,可以添加被控端主机配置文件等。对于一般用户来说,不要随意对其进行更改。在“Configuration Files”面板(如图2所示)中选择“Host Security IDs Files (*.SID)”项,点击“Add”按钮,在上述路径中选择创建好的后缀为“.sid”文件的 Serial ID 文件,将其添加到本安装包中。之后点击“Build”按钮,执行定制版安装 PcAnywhere 的安装包创建动作,之后得到名为“Symantec pcAnywhere.msi”

的安装文件。之后在主机上卸载现有的 PcAnywhere,并安装该定制版 PcAnywhere 安装包。并在所要操作的客户端上安装该定制安装包,就可以利用 Serial ID 验证机制,安全连接 PcAnywhere 被控端了。黑客即使破译了连接密码,因为没有该定制版 PcAnywhere 安装包,是无法连接 PcAnywhere 主机的。

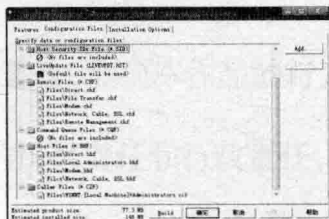
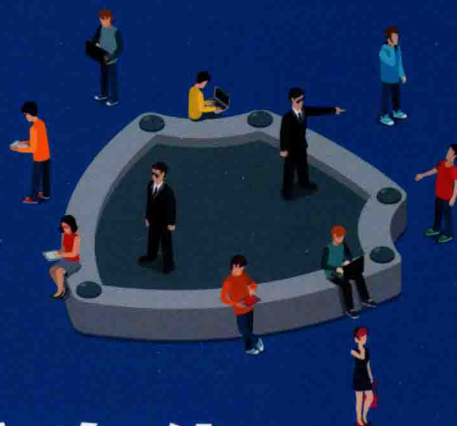


图2 创建自定义安装包

另外,对于使用终端服务的用户来说,为了提高安全性,可以采取相应的安全措施。例如,修改终端服务使用的端口,将其有 3389 修改为别的不常用的端口。这样,当黑客使用 SuperScan 等扫描器扫描 3389 端口时,就可以避免轻易被其发现。为了避免别人随意连接终端服务,最好使用“net user”命令,创建专用的账户,并将其提升到管理员组中。之后在终端服务管理窗口中选择 RDP-Tcp 连接项,在其属性窗口对权限进行调整,删除别的账户,只允许该账户连接终端服务。利用组策略,取消上次远程登录时的账户名称记录信息,禁止显示上次远程登录的账户名等。最关键的是,连接密码必须足够强壮才行。例如,密码长度要达到 12 位以上,内容包括大小写的字母,数字,特殊字符等。而且定期要更换密码,加大黑客破解的难度。这样,当黑客使用 Tscrack 的工具暴力破解密码时,就无法轻易得逞。此外,利用 IPSEC 安全策略和防火墙,可以屏蔽非法 IP,禁止其连接终端服务。这样,即使黑客利用嗅探工具捕获了密码,也无法实施入侵。



网络安全和信息化

2017

超值
精华本

(原《网络运维与管理》)

《网络安全和信息化》(原《网络运维与管理》)是面向网络技术管理人员的实用性刊物。本书是2016年《网络安全和信息化》各期内容的汇集,按照栏目分类进行汇总,内容详尽使用保留价值高。全书分为基础设施管理、系统维护、故障诊断、信息安全4个板块,这些精彩的技术文章,是广大网络管理人员不可多得的业务指导书。

本书读者对象以网络管理技术人员(网管员)为主,辐射网络主管、网络爱好者、准网管员和所有关注网络应用与网络事业发展的人士。



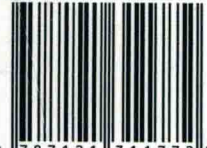
博文视点Broadview



@博文视点Broadview

上架建议: 计算机 > 网管员

ISBN 978-7-121-31177-2



9 787121 311772 >

定价: 89.00元



策划编辑: 符隆美
责任编辑: 徐津平
封面设计: 侯士卿